Red Hat Directory Server 12

配置和架构参考

核心服务器配置属性和服务器架构参考

Last Updated: 2024-07-03

Red Hat Directory Server 12 配置和架构参考

核心服务器配置属性和服务器架构参考

法律通告

摘要

要有效地配置目录服务器部署，了解更多有关核心服务器配置属性的信息，请配置对象类、服务器模式和日志文件。

目录

对红帽文档提供反馈

我们感谢您对文档提供反馈信息。请让我们了解如何改进文档。要做到这一点：

- 要通过 JIRA 提交反馈（需要帐户）：
  1. 登录到 Jira 网站。
  2. 在顶部导航栏中点 **Create**
  3. 在 **Summary** 字段中输入描述性标题。
  4. 在 **Description** 字段中输入您对改进的建议。包括到文档相关部分的链接。
  5. 点对话框底部的 **Create**。
- 要通过 Bugzilla 提交反馈（需要帐户）：
  1. 进入 Bugzilla 网站。
  2. 在 Component 中选择 **Documentation**。
  3. 在 **Description** 中输入您要提供的信息。包括文档相关部分的链接。
  4. 点 **Submit Bug**。

第 1 章 文件位置概述

红帽目录服务器与文件系统层次结构标准(FHS)兼容。有关 FHS 的详情，请参阅 FHS 规格。

1.1. 独立于目录服务器实例的文件和目录

独立于实例的默认文件和目录位置包括：

类型	位置
命令行工具	**/usr/bin/** **/usr/sbin/**
systemd 单元文件	**/usr/lib/systemd/system/dirsrv@.service** **/usr/lib/systemd/system/dirsrv@.service.d/custom.conf** **/usr/lib/systemd/system/dirsrv.target** **/etc/systemd/system/dirsrv.target.wants/**
自签名证书颁发机构	**/etc/dirsrv/ssca**

1.2. 特定于目录服务器实例的文件和目录

为了分隔在同一主机上运行的多个实例，某些文件和目录包含实例的名称。您可以在 Directory 服务器设置过程中设置实例名称。默认情况下，这是没有域名的主机名。例如，如果您的完全限定域名是 **server.example.com**，则默认实例名称为 **server**。

独立于实例的默认文件和目录位置包括：

类型	位置
备份文件	**/var/lib/dirsrv/slapd-*instance_name*/bak/**
配置文件	**/etc/dirsrv/slapd-*instance_name*/**
证书和密钥数据库	**/etc/dirsrv/slapd-*instance_name*/**
数据库文件	**/var/lib/dirsrv/slapd-*instance_name*/db/**
LDIF 文件	**/var/lib/dirsrv/slapd-*instance_name*/ldif/**
锁定文件	**/var/lock/dirsrv/slapd-*instance_name*/**
日志文件	**/var/log/dirsrv/slapd-*instance_name*/**

类型	位置
PID 文件	**/var/run/dirsrv/*instance_name*.pid**
systemd 单元文件	**/etc/systemd/system/dirsrv.target.wants/dirsrv@*instance_name*.service**

1.2.1. 配置文件

每个目录服务器实例将其配置文件存储在 **/etc/dirsrv/slapd-*instance_name*_/** 目录中。

Red Hat Directory Server 的配置信息作为 LDAP 条目存储在 目录中。因此，您必须通过服务器更改服务器配置，而不是编辑配置文件。配置存储的主要优点是，目录管理员可以在服务器仍在运行时使用 LDAP 重新配置服务器，避免需要关闭服务器以进行大多数配置更改。

1.2.2. 目录服务器配置概述

当设置 Directory 服务器时，服务器会将默认配置存储为目录中的一系列 LDAP 条目，位于 **cn=config** 子树下。当您启动服务器时，服务器会从 **dse.ldif** 文件中读取 **cn=config** 子树的内容，该文件采用 LDIF 格式。**dse.ldif** 文件包含所有服务器配置信息，并具有以下名称：

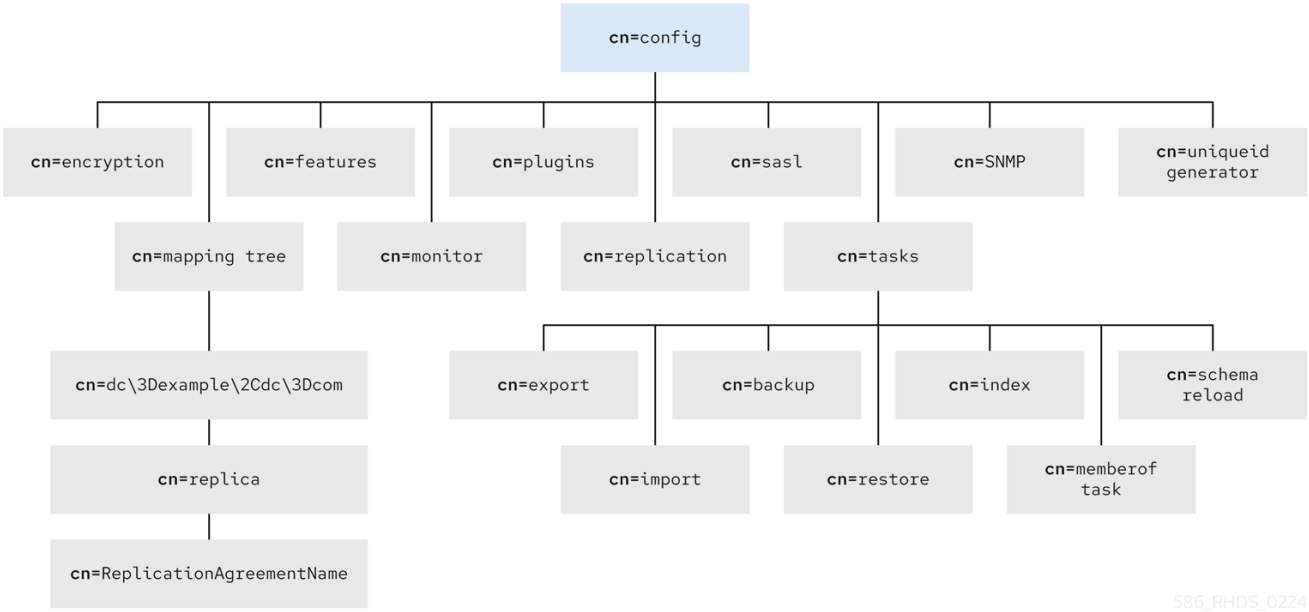
- **se.ldif**.此文件的最新版本。
- **dse.ldif.bak**.最后一次修改前的版本。
- **dse.ldif.startOK**.服务器成功启动的最新文件。

目录服务器的大部分功能都设计为插入到核心服务器的离散模块。每个插件的内部配置的详情包含在 **cn=plugins,cn=config** sub-tree 下的单独条目中。例如，Telephone Syntax 插件的配置包含在 **cn=Telephone Syntax,cn=plugins,cn=config** 中。

同样，特定于数据库的配置存储在 **cn=ldbm database,cn=plugins,cn=config** 下，用于本地数据库，**cn=chaining database,cn=plugins,cn=config** 用于数据库链接。

下图显示了在 **cn=config** 目录树下放置配置数据的位置。

图 1.1. 配置数据子树



dc\3Dexample\2Cdc\3Dcom 值代表 **dc=example,dc=com** DN，带有转义的字符。

1.2.2.1. LDIF 和模式配置文件

目录服务器将配置数据存储在 **/etc/dirsrv/slapd-*instance_name*** 目录中的 LDIF 文件中。如果服务器名称为 **phonebook**，则对于目录服务器，则配置 LDIF 文件都存储在 **/etc/dirsrv/slapd-phonebook** 下。

此目录还包含其他特定于服务器实例的配置文件。

模式配置也以 LDIF 格式存储在以下目录中：

- **/etc/dirsrv/instance_name/schema/** 用于实例特定 schema。
- **/usr/share/dirsrv/schema/** 用于默认模式。
- **/etc/dirsrv/schema/** 用于覆盖默认模式的架构。

注意

在以前的版本中，模式配置文件仅存储在 **/etc/dirsrv/schema** 目录中。

下表列出了提供给 Directory 服务器的配置文件，包括用于兼容服务器模式的配置文件。每个文件前面都有一个数字，它指示应该加载的顺序（以数字顺序排列，然后按字母顺序排列）。

表 1.1. 目录服务器 LDIF 配置文件

配置文件名称	用途
dse.ldif	包含服务器启动时由 目录创建的前端目录特定条目 (DSE)。条目包括 Root DSE (**""**)和 **cn=config** 和 **cn=monitor** (ACIs)的内容。

配置文件名称	用途
00core.ldif	包含 schema 定义，如 **subschemaSubentry**，启动带有最小功能集的服务器（无用户模式，任何非核心功能都没有 schema）。**不要修改此文件**。 用户、特性和应用程序使用的其余架构位于 02common.ldif 文件中，其他架构文件位于 **02common.ldif** 文件中。
02common.ldif	**02common.ldif** 文件包含： ● LDAPv3 标准操作模式，如 **subschemaSubentry**。 ● RFC 2256 中定义的 LDAPv3 标准用户和组织模式（基于 X.520/X.521）。 ● **inetOrgPerson** 和其他广泛使用的属性。 ● 目录服务器配置使用的操作属性。 **修改文件会导致互操作性问题。您必须通过 Directory Server web 控制台** 添加用户定义的属性。
05rfc2247.ldif	来自 RFC 2247 的 schema，*在 LDAP/X500 辨识名称中使用域*，以及相关的 pilot 模式。
05rfc2927.ldif	RFC 2927, *MIME Directory Profile for LDAP Schema* 的 schema。包含要在 **subschema** 子条目中显示的属性所需的 **ldapSchemas** 操作属性。
06inetorgperson.ldif	包含 **01core389.ldif** 模式和 **inetOrgPerson** attribite。
10presence.ldif	传统.schema 用于即时消息存在(online)信息。文件列出了具有必须添加到用户条目中允许的属性的默认对象类，才能为该用户提供即时消息存在信息。
10rfc2307.ldif	RFC 2307 *中的模式，一种将 LDAP 用作网络信息服务的方法*。 当该模式可用时，**10rfc2307bis** 模式(**rfc2307** 的新版本)可能会取代 **10rfc2307.ldif** 方案。
20subscriber.ldif	包含新的模式元素和 Nortel 订阅者互操作性规格。还包含 **adminRole** 和 **memberOf** 属性和 **inetAdmin** 对象类，之前存储在 **50ns-delegated-admin.ldif** 文件中。

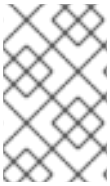
配置文件名称	用途
25java-object.ldif	RFC 2713 *中的模式，用于代表 LDAP 目录中的 Java® 对象*。
28pilot.ldif	包含 RFC 1274 中的 pilot 目录模式，在新部署时不再推荐使用。成功 RFC 1274 的未来 RFC 可能会弃用某些或所有 **28pilot.ldif** 模式属性类型和类。
30ns-common.ldif	包含目录服务器 Web 控制台框架通用的对象类和属性的 schema。
50ns-admin.ldif	红帽管理服务器使用的模式.
50ns-certificate.ldif	Red Hat Certificate Management System 的 schema。
50ns-directory.ldif	包含目录服务器 4.12 和较早版本的目录使用的额外配置模式，它们不再适用于目录服务器的当前版本。这个模式是在 Directory Server 4.12 和当前版本之间的复制。
50ns-mail.ldif	Netscape Messaging 服务器用来定义邮件用户和邮件组的 schema。
50ns-value.ldif	schema 用于 servers 值项目属性。
50ns-web.ldif	Netscape Web 服务器的 schema。
60pam-plugin.ldif	保留供以后使用。
99user.ldif	目录服务器复制消费者维护的用户定义的模式。该架构包含供应商的属性和对象类。

1.2.2.2. **dse.ldif** 服务器配置文件

dse.ldif 文件包含所有配置信息，包括服务器启动时由目录创建的目录特定条目(DSE)，如与数据库相关的条目。该文件包含根目录服务器条目（或 Root DSE，名为 **""**）和 **cn=config** 子树的内容。

当服务器生成 **dse.ldif** 文件时，服务器会按照 **cn=config** 下的目录中显示的顺序列出条目，这通常是对 **cn=config** 基础的 LDAP 搜索子树范围的顺序。

dse.ldif 文件还包含 **cn=monitor** 条目，其主要是只读的，但可以在其上设置 ACI。



注意

dse.ldif 文件不包含 **cn=config** 条目中的每个属性。如果管理员没有设置属性且具有默认值，服务器不会将此属性写入 **dse.ldif** 文件。要查看 **cn=config** 条目中的每个属性，请使用 **ldapsearch** 工具。

配置属性

每个配置条目（如 'cn=config" ）都包含为此条目设置的属性-值对。

以下示例部分 **dse.ldif** 文件显示了通过将 **nsslapd-schemacheck** 属性设置为，从而启用了架构检查。

```
dn: cn=config
objectclass: top
objectclass: extensibleObject
objectclass: nsslapdConfig
nsslapd-accesslog-logging-enabled: on
nsslapd-enquote-sup-oc: off
nsslapd-localhost: phonebook.example.com
nsslapd-schemacheck: on
nsslapd-port: 389
nsslapd-localuser: dirsrv
...
```

配置插件功能

Directory 服务器插件功能的每个部分的配置在 cn=plugins,cn=config 子树下都有自己的独立条目和属性集。

以下示例显示了 Telephone Syntax 插件的示例配置。

```
dn: cn=Telephone Syntax,cn=plugins,cn=config
objectclass: top
objectclass: nsSlapdPlugin
objectclass: extensibleObject
cn: Telephone Syntax
nsslapd-pluginType: syntax
nsslapd-pluginEnabled: on
```

插件配置包含对特定于此插件的所有插件和属性通用的属性。要检查 Directory 服务器当前使用哪些属性，请在 cn=config 子树上运行 ldapsearch 命令。

有关支持的插件及其配置信息的更多信息，请参阅 插件实现服务器功能参考。

配置数据库

cn=UserRoot,cn=ldbm database,cn=plugins,cn=config 子树包含包含默认后缀 Directory 服务器在设置过程中创建的数据库的配置数据。

cn=UserRoot 子树及其子项有许多属性，用来配置不同的数据库设置，如缓存大小、索引文件和事务

日志的路径、用于监控和统计信息的条目和属性，以及数据库索引。

配置索引

索引配置信息作为在以下子目录下的 Directory 服务器中的条目保存：

- cn=index,cn=UserRoot,cn=ldbm database,cn=plugins,cn=config
- cn=default index,cn=config,cn=ldbm database,cn=plugins,cn=config

有关索引的常规信息，请参阅管理索引 文档。

有关索引配置属性的信息，请参阅 cn=config,cn=ldbm database,cn=plugins,cn=config下的数据库属性。

1.2.3. 数据库文件

每个目录服务器实例都包含用于存储所有数据库文件的 /var/lib/dirsrv/slapd-instance/db 目录。/var/lib/dirsrv/slapd-instance/db 目录内容列表示例如下所示。

数据库目录内容

```
db.001 db.002  __db.003  DBVERSION  log.0000000001  userroot/
```

- db.00x 文件.由数据库在内部使用，不得以任何方式移动、删除或修改这些文件。
- log.xxxxxxxxxx 文件。用于存储每个数据库的事务日志。
- DBVERSION.用于存储数据库的版本。

- userroot.存储在设置时创建的用户定义的后缀（用户定义的数据库），如 dc=example,dc=com。

注意

当您创建新数据库（如 testRoot ）时，将目录树存储在新后缀下，名为 testRoot 的目录也会出现在 /var/lib/dirsrv/slapd-instance/db 目录中。

以下示例列出了 userRoot 目录内容。

userroot 数据库目录内容

```
ancestorid.db
DBVERSION
entryrdn.db
id2entry.db
nsuniqueid.db
numsubordinates.db
objectclass.db
parentid.db
```

userroot 子目录包含以下文件：

- ancestorid.db.包含 ID 列表，用于查找条目上级的 ID。
- entrydn.db.包含可用于查找任何 ID 的完整 DN 列表。
- id2entry.db.包含实际目录数据库条目。如果需要，可以从此重新创建所有其他数据库文件。
- nsuniqueid.db.包含用来查找任何 ID 的唯一 ID 列表。

- numsubordinates.db.包含具有子条目的 ID。
- CamelAwsS.db.包含具有特定对象类的 ID 列表。
- parentid.db.包含用于查找父级 ID 的 ID 列表。

1.3. LDIF 文件

目录服务器将 LDIF 相关文件存储在 /usr/share/dirsrv/data/ 目录中。

LDIF 目录内容

```
European.ldif
Example.ldif
Example-roles.ldif
Example-views.ldif
```

示例包含以下文件：

- europe.ldif.包含欧洲字符示例。
- example.ldif.是 LDIF 文件示例。
- example-roles.ldif.是类似 Example.ldif 的 LDIF 文件示例，但它使用角色和类服务，而不是组来为目录管理员设置访问控制和资源限制。

注意

由 db2ldif 或 db2ldif.pl 脚本导出的 LDIF 文件存储在 /var/lib/dirsrv/slapd-*instance_name*/ldif/ 中。

1.4. 锁定文件

每个目录服务器实例包含一个 /var/lock/dirsrv/slapd-*instance_name*/ 目录，用于存储与锁定相关的文件。

以下示例列出了 locks 目录内容。

锁定目录内容

```
exports/ imports/ server/
```

锁定机制控制目录服务器进程可以一次运行多少个副本：

- 如果服务器执行导入，锁定放置在 导入/ 目录中，以防止运行任何其他 ns-slapd （常规）、ldif2db （另一个导入）操作或 db2ldif （导出）操作。
- 如果服务器以正常方式运行，锁定将放置在 server/ 目录中，这只会阻止导入操作。
- 如果服务器执行导出，锁定将放置在 exports/ 目录中。这允许正常服务器操作，但会阻止导入。

可用锁定的数量可能会影响整体目录服务器性能。锁定的数量在 nsslapd-db-locks 属性中设置。如需了解更多详细信息，请参阅 nsslapd-db-locks 属性描述。

1.5. 日志文件

每个目录服务器实例将日志文件存储在 /var/log/dirsrv/slapd-*instance_name*/ 目录中。

日志目录内容

```
access
access.rotationinfo
audit
audit.rotationinfo
errors
errors.rotationinfo
security
security.rotationinfo
```

访问 的内容、审计、错误、安全 日志文件取决于日志配置。stats 文件位于 '/var/run/dirsrv/slapd-*instance_name*.stats/' 目录中。

stats 文件是一个内存映射文件，无法被编辑器读取。它包含 Directory Server SNMP 数据收集组件收集的数据。此数据由 SNMP 子代理读取，以响应 SNMP 属性查询，并与负责处理目录服务器 SNMP 请求的 SNMP 主代理进行通信。

有关所有日志文件的概述，请参阅 日志文件参考 章节。

1.6. PID 文件

当服务器启动并运行时，slapd-serverID.pid 和 slapd-serverID.startpid 文件会在 /var/run/dirsrv/ 目录中创建。这两个文件都存储服务器进程 ID。

1.7. 备份文件

每个目录服务器实例包含以下目录来存储与备份相关的文件：

- /var/lib/dirsrv/slapd-*instance_name*/bak/.包含数据库的备份副本。每个备份都使用数据库备份的实例名称、时间和日期进行日期，例如 *instance_name*-2023_05_04_18_01_23。
- /var/lib/dirsrv/slapd-*instance_name*/bak/config_files/.包含备份的配置文件、证书数据库和自定义架构文件。

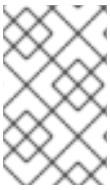
第 2 章 核心服务器配置属性

本节包含与核心服务器功能相关的配置属性的参考信息。有关更改服务器配置的详情，请参考 2.2.1.2 节"访问和修改服务器配置"。有关作为插件实施的服务器功能列表，请参阅 4.1 第 4.1 节"服务器插件功能参考"。有关实现自定义服务器功能的帮助，请联系目录服务器支持。

dse.ldif 文件中存储的配置信息被组织为常规配置条目 cn=config 下的信息树。

以下部分介绍了大多数配置树节点。

cn=plugins 节点在第 4 章介绍，插件实现的服务器功能参考。每个属性的描述包含其目录条目的 DN、其默认值、有效值范围以及其使用示例。



注意

本章中描述的一些条目和属性可能会在以后的版本中有所变化。

2.1. CN=CONFIG

目录服务器在 cn=config 条目中存储常规配置条目。此条目是 nsslapdConfig 对象类的实例，后者从 scalable Object 对象类继承。

2.1.1. nsslapd-accesslog

此属性指定用于记录每个 LDAP 访问的日志的路径和文件名。日志文件中默认记录以下信息：

- 访问数据库的客户端机器的 IP 地址(IPv4 或 IPv6)。
- 执行的操作（如搜索、添加和修改）。
- 访问结果（例如，返回的条目数或错误代码）。

要启用访问日志记录，此属性必须具有有效的 path 和 参数，并且 nsslapd-accesslog-logging-

enabled 配置属性必须在 上 切换到。表列出了这两个配置属性的四个可能值组合，以及禁用或启用访问日志时的结果。

表 2.1. dse.ldif File Attributes

属性	值	启用或禁用日志记录
nsslapd-accesslog-logging-enabled nsslapd-accesslog	on 空字符串	Disabled
nsslapd-accesslog-logging-enabled nsslapd-accesslog	on *filename*	Enabled
nsslapd-accesslog-logging-enabled nsslapd-accesslog	off 空字符串	Disabled
nsslapd-accesslog-logging-enabled nsslapd-accesslog	off *filename*	Disabled

nsslapd-accesslog 参数描述：

参数	描述
条目 DN	cn=config
有效值	任何有效的文件名。
默认值	/var/log/dirsrv/slapd-*instance*/access
语法	DirectoryString
示例	nsslapd-accesslog: /var/log/dirsrv/slapd-*instance*/access

2.1.2. nsslapd-accesslog-compress

默认情况下，目录服务器不会压缩访问日志。将 nsslapd-accesslog-compress 设置为 on，以便在目录服务器轮转日志时启用访问日志压缩。

您不需要重新启动服务器以应用更改。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-accesslog-compress: on

2.1.3. nsslapd-accesslog-level

此属性控制记录到访问日志的内容。

您不必重启服务器才能使此设置生效。

参数	描述
条目 DN	cn=config
有效值	* 0 - 无访问日志 * 4 - 内部访问操作的日志记录 * 256 - 连接、操作和结果的日志 * 512 - 用于访问条目和引用的日志 * 可将这些值添加到一起，以提供所需的准确日志类型；例如，**516** (4 + 512)来获取内部访问操作、条目访问和引用日志。
默认值	256
语法	整数
示例	nsslapd-accesslog-level: 256

2.1.4. nsslapd-accesslog-list

此只读属性（无法设置）提供访问日志轮转中使用的访问日志文件列表。

参数	描述
条目 DN	cn=config
有效值	
默认值	无
语法	DirectoryString
示例	nsslapd-accesslog-list: accesslog2,accesslog3

2.1.5. nsslapd-accesslog-logbuffering

当设置为 **off** 时，服务器会将所有访问日志条目直接写入磁盘。缓冲允许服务器使用访问日志记录，即使负载过重，而不影响性能。但是，在调试时，在禁用缓冲区时，可以立即查看操作及其结果，而不必等待日志条目刷新到文件中。禁用日志缓冲可能会严重影响大量载入的服务器的性能。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	on
语法	DirectoryString
示例	nsslapd-accesslog-logbuffering: off

2.1.6. nsslapd-accesslog-logexpirationtime

此属性指定日志文件在删除前允许达到的最长期限。此属性仅提供单元数量。该单元由 **nsslapd-accesslog-logexpirationtimeunit** 属性提供。

参数	描述
条目 DN	cn=config

参数	描述
有效范围	-1 到最大 32 位整数值(2147483647) 值为 -1 或 0 表示日志永不过期。
默认值	-1
语法	整数
示例	nsslapd-accesslog-logexpirationtime: 2

2.1.7. nsslapd-accesslog-logexpirationtimeunit

此属性指定 nsslapd-accesslog-logexpirationtime 属性的单元。如果服务器未知单元，则日志永远不会过期。

参数	描述
条目 DN	cn=config
有效值	month | 周 | 天
默认值	month
语法	DirectoryString
示例	nsslapd-accesslog-logexpirationtimeunit: week

2.1.8. nsslapd-accesslog-logging-enabled

禁用并启用 accesslog 日志记录，但仅与 nsslapd-accesslog 属性结合使用，用于指定用于记录每个数据库访问的日志的路径和参数。

要启用日志记录，必须在 上 切换到，nsslapd-accesslog 配置属性必须具有有效的 path 和 参数。表列出了这两个配置属性的四个可能值组合，以及禁用或启用访问日志时的结果。

表 2.2. dse.ldif Attributes

属性	值	Logging Enabled 或 Disabled
nsslapd-accesslog-logging-enabled nsslapd-accesslog	on 空字符串	Disabled
nsslapd-accesslog-logging-enabled nsslapd-accesslog	on *filename*	Enabled
nsslapd-accesslog-logging-enabled nsslapd-accesslog	off 空字符串	Disabled
nsslapd-accesslog-logging-enabled nsslapd-accesslog	off *filename*	Disabled

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	on
语法	DirectoryString
示例	nsslapd-accesslog-logging-enabled: off

2.1.9. nsslapd-accesslog-logmaxdiskspace

此属性指定允许使用访问日志的最大磁盘空间量（以 MB 为单位）。如果超过这个值，则会删除最旧的访问日志。

当设置最大磁盘空间时，请考虑可能会因为日志文件轮转而创建的日志文件总数。另外，请记住，目录服务器维护三个不同的日志文件（访问日志、审计日志和错误日志），每个日志文件消耗磁盘空间。将这些注意事项与访问日志的磁盘空间总量进行比较。

参数	描述
条目 DN	cn=config
有效范围	-1 | 1 到最大 32 位整数值(2147483647)，其中值为 -1 表示允许访问日志的磁盘空间的大小没有限制。
默认值	500
语法	整数
示例	nsslapd-accesslog-logmaxdiskspace: 500

2.1.10. nsslapd-accesslog-logminfreediskspace

此属性以 MB 为单位设置允许的最小可用磁盘空间。当可用磁盘空间量低于此属性中指定的值时，将删除最旧的访问日志，直到释放足够的磁盘空间来满足此属性。

参数	描述
条目 DN	cn=config
有效范围	-1 | 1 到最大 32 位整数值(2147483647)
默认值	-1
语法	整数
示例	nsslapd-accesslog-logminfreediskspace: -1

2.1.11. nsslapd-accesslog-logrotationsync-enabled

此属性设定访问日志轮转是否与一天的特定时间同步。以这种方式同步日志轮转，可以在一天（例如每天午夜）的指定时间生成日志文件。这样可以更轻松地分析日志文件，因为它们然后直接映射到日历。

要使访问日志轮转与时间同步，必须使用 nsslapd-accesslog-logrotationsynchour 和 nsslapd-accesslog-logrotationsyncmin 属性值设置为轮转日志文件的时间和分钟。

例如，要每天在午夜轮转访问日志文件，请通过在 上 将其值设置为，然后将 nsslapd-accesslog-logrotationsynchour 和 nsslapd-accesslog-logrotationsyncmin 属性设为 0 来启用此属性。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-accesslog-logrotationsync-enabled: on

2.1.12. nsslapd-accesslog-logrotationsynchour

此属性设置轮转访问日志的天数。此属性必须与 nsslapd-accesslog-logrotationsync-enabled 和 nsslapd-accesslog-logrotationsyncmin 属性一起使用。

参数	描述
条目 DN	cn=config
有效范围	0 到 23
默认值	0
语法	整数
示例	nsslapd-accesslog-logrotationsynchour: 23

2.1.13. nsslapd-accesslog-logrotationsyncmin

此属性设置轮转访问日志的当天的分钟。此属性必须与 nsslapd-accesslog-logrotationsync-enabled 和 nsslapd-accesslog-logrotationsynchour 属性一起使用。

参数	描述
条目 DN	cn=config
有效范围	0 到 59
默认值	0

参数	描述
语法	整数
示例	nsslapd-accesslog-logrotationsyncmin: 30

2.1.14. nsslapd-accesslog-logrotationtime

此属性设置访问日志文件轮转之间的时间。此属性仅提供单元数量。单位（天、每周、月份等）由 nsslapd-accesslog-logrotationtimeunit 属性提供。

目录服务器在配置的时间间隔到期后，在第一次写入操作时轮转日志，而不考虑日志的大小。

虽然不建议以性能原因来指定日志轮转，因为日志无限期增长，但可以通过两种方式指定此功能。将 nsslapd-accesslog-maxlogsperdir 属性值设置为 1，或者将 nsslapd-accesslog-logrotationtime 属性设置为 -1。服务器首先检查 nsslapd-accesslog-maxlogsperdir 属性，如果此属性值大于 1，则服务器会检查 nsslapd-accesslog-logrotationtime 属性。请参阅 第 2.1.17 节 “nsslapd-accesslog-maxlogsperdir” 了解更多信息。

参数	描述
条目 DN	cn=config
有效范围	-1	1 到最大 32 位整数值(2147483647)，其中值为 -1 表示访问日志文件轮转之间的时间没有限制。
默认值	1
语法	整数
示例	nsslapd-accesslog-logrotationtime: 100

2.1.15. nsslapd-accesslog-logrotationtimeunit

此属性设置 nsslapd-accesslog-logrotationtime 属性的单元。

参数	描述
条目 DN	cn=config

参数	描述
有效值	month | week | day | hour | minute
默认值	day
语法	DirectoryString
示例	nsslapd-accesslog-logrotationtimeunit: week

2.1.16. nsslapd-accesslog-maxlogsize

此属性以 MB 为单位设置最大访问日志大小。当达到这个值时，访问日志会被轮转。这意味着服务器开始向新日志文件写入日志信息。如果 nsslapd-accesslog-maxlogsperdir 属性设置为 1，服务器会忽略此属性。

在设置最大日志大小时，请考虑以下几点：

- 由于日志文件轮转，可以创建的日志文件总数。
- 目录服务器维护五个不同的日志文件：访问日志、审计日志、审计失败日志、错误日志、安全日志。每个日志文件都会消耗磁盘空间。

将这些注意事项与您要为访问日志设置的磁盘空间总量进行比较。

参数	描述
条目 DN	cn=config
有效范围	-1 | 1 到最大 32 位整数值(2147483647)，其中值为 -1 表示日志文件的大小没有限制。
默认值	100
语法	整数
示例	nsslapd-accesslog-maxlogsize: 100

2.1.17. nsslapd-accesslog-maxlogsperdir

此属性设置存储了访问日志的目录中的访问日志总数。每次轮转访问日志时，都会创建一个新的日志文件。当访问日志目录中包含的文件数量超过此属性中存储的值时，会删除日志文件的最老版本。出于性能原因，请不要将此值设置为 1，因为服务器不会轮转日志，并且会无限期地增长。

如果此属性的值大于 1，请检查 nsslapd-accesslog-logrotationtime 属性来建立是否指定了日志轮转。如果 nsslapd-accesslog-logrotationtime 属性的值为 -1，则没有日志轮转。请参阅 第 2.1.14 节 “nsslapd-accesslog-logrotationtime” 了解更多信息。

根据 nsslapd-accesslog-logminfreediskspace 和 nsslapd-accesslog-maxlogsize 中设置的值，实际日志数量可能小于您在 nsslapd-accesslog-maxlogsperdir 中配置的内容。例如，如果 nsslapd-accesslog-maxlogsperdir 使用默认值(10 文件)，并将 nsslapd-accesslog-logminfreediskspace 设置为 500 MB，nsslapd-accesslog-maxlogsize 只保留 5 个访问日志文件。

参数	描述
条目 DN	cn=config
有效范围	1 到最大 32 位整数值(2147483647)
默认值	10
语法	整数
示例	nsslapd-accesslog-maxlogsperdir: 10

2.1.18. nsslapd-accesslog-mode

此属性设置创建访问日志文件的访问模式或文件权限。有效值是 000 到 777 (它们镜像编号或绝对 UNIX 文件权限)的组合。该值必须是 3 位数字，数字因 0 到 7 的不同：

- 0 - None
- 1 - 只执行
- 2 - 仅写入
- 3 - 写入和执行

- **4 - 只读**
- **5 - 读取和执行**
- **6 - 读取和写入**
- **7 - 读、写和执行**

在 3 位数字中，第一个数字代表所有者的权限，第二个数字代表组的权限，第三个数字代表每个人的权限。更改默认值时，请记住 000 不允许访问日志，并且允许每个人的写入权限都可能导致日志被任何人覆盖或删除。

新配置的访问模式只会影响创建的新日志；当日志轮转到新文件时，会设置模式。

参数	描述
条目 DN	cn=config
有效范围	000 到 777
默认值	600
语法	整数
示例	nsslapd-accesslog-mode: 600

2.1.19. nsslapd-allow-anonymous-access

如果用户尝试在不提供任何绑定 DN 或密码的情况下尝试连接到目录服务器，则这是 *匿名绑定*。匿名绑定简化了常见的搜索和读取操作，例如，通过不要求用户先向目录进行身份验证，例如检查电话号码或电子邮件地址的目录。

但是，匿名绑定存在风险。适当的 ACI 必须就位才能限制对敏感信息的访问以及禁止修改和删除等操作。此外，匿名绑定可用于拒绝服务攻击或恶意人员获得对服务器的访问。

可以禁用匿名绑定以提高安全性(off)。默认情况下，允许匿名绑定(on)搜索和读取操作。这样可以访问

常规目录条目，其中包括用户和组条目，以及 root DSE 等配置条目。第三个选项 rootdse 允许匿名搜索和读取访问权限来搜索 root DSE 本身，但限制对所有其他目录条目的访问。

另外，也可以使用 nsslapd-anonlimitsdn 属性将资源限值放在匿名绑定上，如 第 2.1.23 节 “nsslapd-anonlimitsdn” 所述。

对这个值的更改不会生效，直到服务器重启为止。

参数	描述
条目 DN	cn=config
有效值	on | off | rootdse
默认值	on
语法	DirectoryString
示例	nsslapd-allow-anonymous-access: on

2.1.20. nsslapd-allowed-sasl-mechanisms

默认情况下，root DSE 列出 SASL 库支持的所有机制。但是，在某些环境中，首选使用某些环境。nsslapd-allowed-sasl-mechanisms 属性允许您只启用一些定义的 SASL 机制。

机制名称必须包含大写字母、数字和下划线。每个机制可以使用逗号或空格分开。

注意

EXTERNAL 机制实际上没有被任何 SASL 插件使用。它是服务器内部的，主要用于 TLS 客户端身份验证。因此，EXTERNAL 机制无法被限制或控制。它始终会出现在支持的机制列表中，无论 nsslapd-allowed-sasl-mechanisms 属性中设置什么。

此设置不需要重启服务器才能生效。

参数	描述
条目 DN	cn=config
有效值	任何有效的 SASL 机制
默认值	none （允许的所有 SASL 机制）
语法	DirectoryString
示例	nsslapd-allowed-sasl-mechanisms: GSSAPI, DIGEST-MD5, OTP

2.1.21. nsslapd-allow-hashed-passwords

这个参数禁用预哈希密码检查。默认情况下，Directory 服务器不允许由 Directory Manager 以外的任何人设置预哈希密码。当您将这个特权添加到 Password Administrators 组时，您可以将这个特权委派给其他用户。然而，在某些情况下，如复制合作伙伴已经控制预哈希密码检查时，必须在 Directory 服务器上禁用此功能。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-allow-hashed-passwords: off

2.1.22. nsslapd-allow-unauthenticated-binds

未经身份验证的绑定是用户提供空密码的目录服务器的连接。使用默认设置，出于安全原因，Directory 服务器拒绝在此场景中的访问。

警告

红帽建议不要启用未经身份验证的绑定。这个验证方法允许用户在不以任何帐户形式提供密码的情况下绑定，包括 Directory Manager。绑定后，用户可以使用用于绑定的帐户的权限访问所有数据。

您不必重启服务器才能使此设置生效。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-allow-unauthenticated-binds: off

2.1.23. nsslapd-anonlimitsdn

可以在经过身份验证的绑定上设置资源限值。资源限值可以设置可在单个操作中搜索多少个条目(nsslapd-sizeLimit)、时间限制(nsslapd-timelimit)和超时周期(nsslapd-idletimeout)用于搜索，以及可以搜索的条目总数(nsslapd-lookthroughlimit)。这些资源限制可防止拒绝服务攻击访问目录资源并改进整体性能。

在用户条目上设置资源限值。匿名绑定（明显）没有与之关联的用户条目。这意味着资源限值通常不适用于匿名操作。

要为匿名绑定设置资源限值，可以创建一个模板条目，并带有适当的资源限值。然后，可以添加 nsslapd-anonlimitsdn 配置属性来指向此条目，并将资源限值应用到匿名绑定。

参数	描述
条目 DN	cn=config

参数	描述
有效值	任何 DN
默认值	无
语法	DirectoryString
示例	nsslapd-anonlimitsdn: cn=anon template,ou=people,dc=example,dc=com

2.1.24. nsslapd-attribute-name-exceptions

此属性允许属性名称中的非标准字符用于向后兼容旧的服务器，如 schema 定义的属性中的 "_"。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-attribute-name-exceptions: on

2.1.25. nsslapd-auditfaillog

此属性设置用于记录失败的 LDAP 修改的日志的路径和文件名。

如果启用了 nsslapd-auditfaillog-logging-enabled，并且未设置 nsslapd-auditfaillog，则审计失败事件会记录到 nsslapd-auditlog 中指定的文件。

如果将 nsslapd-auditfaillog 参数设置为与 nsslapd-auditlog 相同的路径，则这两者都会记录到同一文件中。

参数	描述
条目 DN	cn=config

参数	描述
有效值	任何有效的文件名
默认值	/var/log/dirsrv/slapd-*instance*/audit
语法	DirectoryString
示例	nsslapd-auditfaillog: /var/log/dirsrv/slapd-*instance*/audit

要启用审计失败日志，此属性必须具有有效的路径，并且 nsslapd-auditfaillog-logging-enabled 属性必须设置为 on

2.1.26. nsslapd-auditfaillog-compress

默认情况下，目录服务器不会压缩审计失败日志。将 nsslapd-auditfaillog-compress 设置为 on，以便在 Directory 服务器轮转日志时启用审计失败日志压缩。

您不需要重新启动服务器以应用更改。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-auditfaillog-compress: on

2.1.27. nsslapd-auditfaillog-list

提供审计失败日志文件列表。

参数	描述

参数	描述
条目 DN	cn=config
有效值	
默认值	无
语法	DirectoryString
示例	nsslapd-auditfaillog-list: auditfaillog2,auditfaillog3

2.1.28. nsslapd-auditfaillog-logexpirationtime

此属性设置日志文件在删除前的最长期限。它为单位数提供。在 nsslapd-auditfaillog-logexpirationtimeunit 属性中指定单位，如 day, week, month 等。

参数	描述
条目 DN	cn=config
有效范围	-1 到最大 32 位整数值(2147483647) 值为 -1 或 0 表示日志永不过期。
默认值	-1
语法	整数
示例	nsslapd-auditfaillog-logexpirationtime: 1

2.1.29. nsslapd-auditfaillog-logexpirationtimeunit

此属性设置 nsslapd-auditfaillog-logexpirationtime 属性的单元。如果服务器未知单元，日志永远不会过期。

参数	描述
条目 DN	cn=config
有效值	month | 周 | 天
默认值	week

参数	描述
语法	DirectoryString
示例	nsslapd-auditfaillog-logexpirationtimeunit: day

2.1.30. nsslapd-auditfaillog-logging-enabled

打开和关闭失败的 LDAP 修改的日志。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-auditfaillog-logging-enabled: off

2.1.31. nsslapd-auditfaillog-logmaxdiskspace

此属性设置审计日志可以使用的最大磁盘空间量，以 MB 为单位。如果大小超过限制，则删除最旧的审计日志。

参数	描述
条目 DN	cn=config
有效范围	-1 | 1 到最大 32 位整数值(2147483647)，其中值为 -1 表示允许审计失败的磁盘空间大小没有限制。
默认值	100
语法	整数
示例	nsslapd-auditfaillog-logmaxdiskspace: 10000

2.1.32. nsslapd-auditfaillog-logminfreediskspace

此属性以 MB 为单位设置允许的最小可用磁盘空间。当可用磁盘空间量低于指定的值时，将删除最旧的审计日志，直到释放足够的磁盘空间。

参数	描述
条目 DN	cn=config
有效范围	-1 (unlimited)| 1 到最大 32 位整数值(2147483647)
默认值	-1
语法	整数
示例	nsslapd-auditfaillog-logminfreediskspace: -1

2.1.33. nsslapd-auditfaillog-logrotationsync-enabled

此属性设定审计日志轮转是否与一天的特定时间同步。以这种方式同步日志轮转，可以在一天（例如每天午夜）的指定时间生成日志文件。这样可以更轻松地分析日志文件，因为它们然后直接映射到日历。

要使审计日志轮转与时间同步，必须使用 nsslapd-auditfaillog-logrotationsynchour 和 nsslapd-auditfaillog-logrotationsyncmin 属性值设置为轮转日志文件的时间和分钟。

例如，要每天在午夜轮转审计失败日志文件，请通过在 上 将其值设置为，然后将 nsslapd-auditfaillog-logrotationsynchour 和 nsslapd-auditfaillog-logrotationsyncmin 属性设为 0 来启用此属性。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-auditfaillog-logrotationsync-enabled: on

2.1.34. nsslapd-auditfaillog-logrotationsynchour

此属性设置审计日志轮转天数的小时。此属性必须与 **nsslapd-auditfaillog-logrotationsync-enabled** 和 **nsslapd-auditfaillog-logrotationsyncmin** 属性一起使用。

参数	描述
条目 DN	cn=config
有效范围	0 到 23
默认值	none （因为 **nsslapd-auditfaillog-logrotationsync-enabled** 为 off）
语法	整数
示例	nsslapd-auditfaillog-logrotationsynchour: 23

2.1.35. nsslapd-auditfaillog-logrotationsyncmin

此属性设置审计失败日志轮转的时间。此属性必须与 **nsslapd-auditfaillog-logrotationsync-enabled** 和 **nsslapd-auditfaillog-logrotationsynchour** 属性一起使用。

参数	描述
条目 DN	cn=config
有效范围	0 到 59
默认值	none （因为 **nsslapd-auditfaillog-logrotationsync-enabled** 为 off）
语法	整数
示例	nsslapd-auditfaillog-logrotationsyncmin: 30

2.1.36. nsslapd-auditfaillog-logrotationtime

此属性设置审计日志文件轮转之间的时间。此属性仅提供单元数量。单位（天、每周、月份等）由 **nsslapd-auditfaillog-logrotationtimeunit** 属性提供。如果 **nsslapd-auditfaillog-maxlogsperdir** 属性设置为 **1**，服务器会忽略此属性。

目录服务器在配置的时间间隔到期后，在第一次写入操作时轮转日志，而不考虑日志的大小。

虽然不建议指定日志轮转的性能原因，但随着日志无限期增长，但可以通过两种方式指定此功能。将 **nsslapd-auditfaillog-maxlogsperdir** 属性值设为 **1**，或者将 **nsslapd-auditfaillog-logrotationtime** 属性设置为 **-1**。服务器首先检查 **nsslapd-auditfaillog-maxlogsperdir** 属性，如果此属性值大于 **1**，则服务器会检查 **nsslapd-auditfaillog-logrotationtime** 属性。请参阅 第 2.1.25 节 “nsslapd-auditfaillog” 了解更多信息。

参数	描述
条目 DN	cn=config
有效范围	-1	1 到最大 32 位整数值(2147483647)，其中 -1 表示审计失败日志文件轮转之间的时间没有限制。
默认值	1
语法	整数
示例	nsslapd-auditfaillog-logrotationtime: 100

2.1.37. nsslapd-auditfaillog-logrotationtimeunit

此属性设置 **nsslapd-auditfaillog-logrotationtime** 属性的单元。

参数	描述
条目 DN	cn=config
有效值	month | week | day | hour | minute
默认值	week
语法	DirectoryString
示例	nsslapd-auditfaillog-logrotationtimeunit: day

2.1.38. nsslapd-auditfaillog-maxlogsize

此属性以 **MB** 为单位设置最大审计日志大小。当达到这个值时，审计失败日志会被轮转。这意味着服务器开始向新日志文件写入日志信息。如果 **nsslapd-auditfaillog-maxlogsperdir** 参数设置为 **1**，服务器会忽略此属性。

参数	描述
条目 DN	cn=config
有效范围	-1 | 1 到最大 32 位整数值(2147483647)，其中值为 -1 表示日志文件的大小没有限制。
默认值	100
语法	整数
示例	nsslapd-auditfaillog-maxlogsize: 50

2.1.39. nsslapd-auditfaillog-maxlogsperdir

此属性设置可包含在审计日志的目录中的审计日志总数。每次轮转审计失败日志时，都会创建新的日志文件。当审计日志目录中包含的文件数量超过此属性中存储的值时，会删除日志文件的最老版本。默认值为 1 日志。如果接受此默认值，服务器将不会轮转日志，它会无限期地增长。

如果此属性的值大于 1，请检查 nsslapd-auditfaillog-logrotationtime 属性来建立是否指定了日志轮转。如果 nsslapd-auditfaillog-logrotationtime 属性的值为 -1，则没有日志轮转。请参阅 第 2.1.28 节 “nsslapd-auditfaillog-logexpirationtime” 了解更多信息。

参数	描述
条目 DN	cn=config
有效范围	1 到最大 32 位整数值(2147483647)
默认值	1
语法	整数
示例	nsslapd-auditfaillog-maxlogsperdir: 10

2.1.40. nsslapd-auditfaillog-mode

此属性设置创建审计日志文件的访问模式或文件权限。有效值是 000 到 777 的组合，因为它们镜像编号或绝对 UNIX 文件权限。该值必须是 3 位数字的组合，数字因 0 到 7 的不同：

- 0 - None

- 1 - 只执行
- 2 - 仅写入
- 3 - 写入和执行
- 4 - 只读
- 5 - 读取和执行
- 6 - 读取和写入
- 7 - 读、写和执行

在 3 位数字中，第一个数字代表所有者的权限，第二个数字代表组的权限，第三个数字代表每个人的权限。更改默认值时，请记住 000 不允许访问日志，并且允许每个人的写入权限都可能导致日志被任何人覆盖或删除。

新配置的访问模式只会影响创建的新日志；当日志轮转到新文件时，会设置模式。

参数	描述
条目 DN	cn=config
有效范围	000 到 777
默认值	600
语法	整数
示例	nsslapd-auditfaillog-mode: 600

2.1.41. nsslapd-auditlog

此属性设置日志的路径和文件名，用于记录对每个数据库所做的更改。

参数	描述
条目 DN	cn=config
有效值	任何有效的文件名
默认值	/var/log/dirsrv/slapd-*instance*/audit
语法	DirectoryString
示例	nsslapd-auditlog: /var/log/dirsrv/slapd-*instance*/audit

要使审计日志记录启用，此属性必须具有有效的 path 和 参数，并且 nsslapd-auditlog-logging-enabled 配置属性必须在 上 切换到。表列出了这两个配置属性的四个可能值组合，以及它们的结果在禁用或启用审计日志记录方面的结果。

表 2.3. nsslapd-auditlog 的可能组合

dse.ldif 中的属性	值	启用或禁用日志记录
nsslapd-auditlog-logging-enabled nsslapd-auditlog	on 空字符串	Disabled
nsslapd-auditlog-logging-enabled nsslapd-auditlog	on *filename*	Enabled
nsslapd-auditlog-logging-enabled nsslapd-auditlog	off 空字符串	Disabled
nsslapd-auditlog-logging-enabled nsslapd-auditlog	off *filename*	Disabled

2.1.42. nsslapd-auditlog-display-attrs

使用 nsslapd-auditlog-display-attrs 属性，您可以设置目录服务器在审计日志中显示的属性，以提供有关被修改条目的有用识别信息。通过在审计日志中添加属性，您可以检查条目中特定属性的当前状态以及条目更新的详情。

您可以通过选择以下选项之一来显示日志中的属性：

- 要显示 Directory 服务器修改的条目的特定属性，请将属性名称作为值提供。
- 要显示多个属性，请提供以空格分隔的属性名称列表作为值。
- 要显示条目的所有属性，请使用星号 packagemanifests 作为值。

提供目录服务器在审计日志中必须显示的属性列表，或使用星号(*)作为值来显示被修改的条目的所有属性。

例如，要将 cn 属性添加到审计日志输出中，请将 nsslapd-auditlog-display-attrs 属性设置为 cn。审计日志包含类似如下的条目：

```
time: 20221027102743
dn: uid=73747737483,ou=people,dc=example,dc=com
#cn: John Smith
result: 0
changetype: modify
...
```

参数	描述
条目 DN	cn=config
有效值	任何有效的属性 name 和星号(*)
默认值	无
语法	DirectoryString
示例	nsslapd-auditlog-display-attrs: cn ou

2.1.43. nsslapd-auditlog-compress

默认情况下，目录服务器不会压缩审计日志。将 nsslapd-auditlog-compress 设置为 on，以便在目录服务器轮转日志时启用审计日志压缩。

您不需要重新启动服务器以应用更改。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-auditlog-compress: on

2.1.44. nsslapd-auditlog-list

提供审计日志文件列表。

参数	描述
条目 DN	cn=config
有效值	
默认值	无
语法	DirectoryString
示例	nsslapd-auditlog-list: auditlog2,auditlog3

2.1.45. nsslapd-auditlog-logexpirationtime

此属性设置在删除日志文件前允许的日志文件的最长期限。此属性仅提供单元数量。单位（天、每周、月份等）由 nsslapd-auditlog-logexpirationtimeunit 属性提供。

参数	描述
条目 DN	cn=config

参数	描述
有效范围	-1 到最大 32 位整数值(2147483647) 值为 -1 或 0 表示日志永不过期。
默认值	-1
语法	整数
示例	nsslapd-auditlog-logexpirationtime: 1

2.1.46. nsslapd-auditlog-logexpirationtimeunit

此属性设置 nsslapd-auditlog-logexpirationtime 属性的单元。如果服务器未知单元，则日志永远不会过期。

参数	描述
条目 DN	cn=config
有效值	month | 周 | 天
默认值	week
语法	DirectoryString
示例	nsslapd-auditlog-logexpirationtimeunit: day

2.1.47. nsslapd-auditlog-logging-enabled

打开和关闭审计日志记录。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString

参数	描述
示例	nsslapd-auditlog-logging-enabled: off

要使审计日志记录启用，此属性必须具有有效的 path 和 参数，并且 nsslapd-auditlog-logging-enabled 配置属性必须切换到。表列出了这两个配置属性的四个可能值组合，以及它们的结果在禁用或启用审计日志记录方面的结果。

表 2.4. nsslapd-auditlog 和 nsslapd-auditlog-logging-enabled 的可能组合

属性	值	启用或禁用日志记录
nsslapd-auditlog-logging-enabled nsslapd-auditlog	on 空字符串	Disabled
nsslapd-auditlog-logging-enabled nsslapd-auditlog	on *filename*	Enabled
nsslapd-auditlog-logging-enabled nsslapd-auditlog	off 空字符串	Disabled
nsslapd-auditlog-logging-enabled nsslapd-auditlog	off *filename*	Disabled

2.1.48. nsslapd-auditlog-logmaxdiskspace

此属性设置审计日志允许使用的最大磁盘空间量，以 MB 为单位。如果超过这个值，则会删除最旧的审计日志。

当设置最大磁盘空间时，请考虑可能会因为日志文件轮转而创建的日志文件总数。还请记住，目录服务器维护三个不同的日志文件（访问日志、审计日志和错误日志），各自消耗磁盘空间。将这些注意事项与审计日志的磁盘空间总量进行比较。

参数	描述
条目 DN	cn=config
有效范围	-1	1 到 32 位整数值(2147483647)，其中值为 -1 表示审计日志的磁盘空间的大小没有限制。

参数	描述
默认值	-1
语法	整数
示例	nsslapd-auditlog-logmaxdiskspace: 10000

2.1.49. nsslapd-auditlog-logminfreediskspace

此属性以 MB 为单位设置允许的最小可用磁盘空间。当可用磁盘空间量低于此属性指定的值时，将删除最旧的审计日志，直到有足够的磁盘空间来满足此属性。

参数	描述
条目 DN	cn=config
有效范围	-1 (unlimited)| 1 到最大 32 位整数值(2147483647)
默认值	-1
语法	整数
示例	nsslapd-auditlog-logminfreediskspace: -1

2.1.50. nsslapd-auditlog-logrotationsync-enabled

此属性设定审计日志轮转是否与一天的特定时间同步。以这种方式同步日志轮转，可以在一天（例如每天午夜）的指定时间生成日志文件。这样可以更轻松地分析日志文件，因为它们然后直接映射到日历。

要使审计日志轮转与时间同步，必须使用 nsslapd-auditlog-logrotationsynchour 和 nsslapd-auditlog-logrotationsyncmin 属性值启用此属性。

例如，要每天在午夜轮转审计日志文件，请通过在 上 将其值设置为，然后将 nsslapd-auditlog-logrotationsynchour 和 nsslapd-auditlog-logrotationsyncmin 属性设为 0 来启用此属性。

参数	描述
条目 DN	cn=config

参数	描述
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-auditlog-logrotationsync-enabled: on

2.1.51. nsslapd-auditlog-logrotationsynchour

此属性设置轮转审计日志的日期的小时。此属性必须与 nsslapd-auditlog-logrotationsync-enabled 和 nsslapd-auditlog-logrotationsyncmin 属性一起使用。

参数	描述
条目 DN	cn=config
有效范围	0 到 23
默认值	none （因为 **nsslapd-auditlog-logrotationsync-enabled** 为 off）
语法	整数
示例	nsslapd-auditlog-logrotationsynchour: 23

2.1.52. nsslapd-auditlog-logrotationsyncmin

此属性设置轮转审计日志的日期的分钟数。此属性必须与 nsslapd-auditlog-logrotationsync-enabled 和 nsslapd-auditlog-logrotationsynchour 属性一起使用。

参数	描述
条目 DN	cn=config
有效范围	0 到 59
默认值	none （因为 **nsslapd-auditlog-logrotationsync-enabled** 为 off）

参数	描述
语法	整数
示例	nsslapd-auditlog-logrotationsyncmin: 30

2.1.53. nsslapd-auditlog-logrotationtime

此属性设置审计日志文件轮转之间的时间。此属性仅提供单元数量。单位（天、每周、月份等）由 nsslapd-auditlog-logrotationtimeunit 属性提供。如果 nsslapd-auditlog-maxlogsperdir 属性设置为 1，服务器会忽略此属性。

目录服务器在配置的时间间隔到期后，在第一次写入操作时轮转日志，而不考虑日志的大小。

虽然不建议指定日志轮转的性能原因，但随着日志无限期增长，但可以通过两种方式指定此功能。将 nsslapd-auditlog-maxlogsperdir 属性值设置为 1，或者将 nsslapd-auditlog-logrotationtime 属性设置为 -1。服务器首先检查 nsslapd-auditlog-maxlogsperdir 属性，如果此属性值大于 1，则服务器会检查 nsslapd-auditlog-logrotationtime 属性。请参阅 第 2.1.39 节 “nsslapd-auditfaillog-maxlogsperdir” 了解更多信息。

参数	描述
条目 DN	cn=config
有效范围	-1 | 1 到最大 32 位整数值(2147483647)，其中值为 -1 表示审计日志文件轮转之间的时间没有限制。
默认值	1
语法	整数
示例	nsslapd-auditlog-logrotationtime: 100

2.1.54. nsslapd-auditlog-logrotationtimeunit

此属性设置 nsslapd-auditlog-logrotationtime 属性的单元。

参数	描述
条目 DN	cn=config

参数	描述
有效值	month | week | day | hour | minute
默认值	week
语法	DirectoryString
示例	nsslapd-auditlog-logrotationtimeunit: day

2.1.55. nsslapd-auditlog-maxlogsize

此属性以 MB 为单位设置最大审计日志大小。当达到这个值时，审计日志会被轮转。这意味着服务器开始向新日志文件写入日志信息。如果 nsslapd-auditlog-maxlogsperdir 到 1，服务器会忽略此属性。

在设置最大日志大小时，请考虑可能会因为日志文件轮转而创建的日志文件总数。另外，请记住，Directory 服务器维护五个不同的日志文件（访问日志、审计日志、审计日志、错误日志、安全日志），每个日志文件消耗磁盘空间。将这些注意事项与审计日志的磁盘空间总量进行比较。

参数	描述
条目 DN	cn=config
有效范围	-1 | 1 到最大 32 位整数值(2147483647)，其中值为 -1 表示日志文件的大小没有限制。
默认值	100
语法	整数
示例	nsslapd-auditlog-maxlogsize: 50

2.1.56. nsslapd-auditlog-maxlogsperdir

此属性设置可包含审计日志的审计日志总数。每次轮转审计日志时，都会创建一个新的日志文件。当审计日志目录中包含的文件数量超过此属性中存储的值时，会删除日志文件的最老版本。默认值为 1 日志。如果接受此默认值，服务器将不会轮转日志，它会无限期地增长。

如果此属性的值大于 1，请检查 nsslapd-auditlog-logrotationtime 属性来建立是否指定了日志轮转。如果 nsslapd-auditlog-logrotationtime 属性的值为 -1，则没有日志轮转。请参阅 第 2.1.14 节 “nsslapd-accesslog-logrotationtime” 了解更多信息。

参数	描述
条目 DN	cn=config
有效范围	1 到最大 32 位整数值(2147483647)
默认值	1
语法	整数
示例	nsslapd-auditlog-maxlogsperdir: 10

2.1.57. nsslapd-auditlog-mode

此属性设置创建审计日志文件的访问模式或文件权限。有效值是 000 到 777 的组合，因为它们镜像编号或绝对 UNIX 文件权限。该值必须是 3 位数字的组合，数字因 0 到 7 的不同：

- 0 - None
- 1 - 只执行
- 2 - 仅写入
- 3 - 写入和执行
- 4 - 只读
- 5 - 读取和执行
- 6 - 读取和写入
- 7 - 读、写和执行

在 3 位数字中，第一个数字代表所有者的权限，第二个数字代表组的权限，第三个数字代表每个人的

权限。更改默认值时，请记住 000 不允许访问日志，并且允许每个人的写入权限都可能导致日志被任何人覆盖或删除。

新配置的访问模式只会影响创建的新日志；当日志轮转到新文件时，会设置模式。

参数	描述
条目 DN	cn=config
有效范围	000 到 777
默认值	600
语法	整数
示例	nsslapd-auditlog-mode: 600

2.1.58. nsslapd-bakdir

此参数设置默认备份目录的路径。Directory Server 用户必须在配置的目录中具有写入权限。

此设置不需要重启服务器才能生效。

参数	描述
条目 DN	cn=config
有效值	任何本地目录路径。
默认值	/var/lib/dirsrv/slapd-*instance*/bak
语法	DirectoryString
示例	nsslapd-bakdir: /var/lib/dirsrv/slapd-*instance*/bak

2.1.59. nsslapd-certdir

此参数定义目录服务器用于存储实例的网络安全服务(NSS)数据库的目录的完整路径。此数据库包含实例的私钥和证书。

作为回退，如果服务器无法将它们提取到私有命名空间中的 /tmp/ 目录中，则目录服务器会将私钥和证书提取到这个目录中。有关私有命名空间的详情，请查看 ***systemd.exec (5)*** 手册页中的 **PrivateTmp** 参数描述。

nsslapd-certdir 中指定的目录必须由服务器的用户 **ID** 所有，且只有此用户 **ID** 在这个目录中必须具有读写权限。为安全起见，其他用户不应具有读取或写入到此目录的权限。

必须重启该服务才能使此属性生效。

参数	描述
条目 DN	cn=config
有效值	绝对路径
默认值	/etc/dirsrv/slapd-*instance_name*/
语法	DirectoryString
示例	nsslapd-certdir: /etc/dirsrv/slapd-*instance_name*/

2.1.60. nsslapd-certmap-basedn

当使用 TLS 证书执行客户端身份验证时，可以使用此属性，以避免在 **/etc/dirsrv/slapd-*instance_name*/certmap.conf** 文件中配置的安全子系统证书映射的限制。根据此文件中的配置，证书映射可以使用基于根 DN 的目录子树搜索来完成。如果搜索基于根 DN，则 **nsslapd-certmap-basedn** 属性可能会强制搜索基于 root 以外的一些条目。此属性的有效值是用于证书映射的后缀或子树的 DN。

参数	描述
条目 DN	cn=config
有效值	任何有效的 DN
默认值	
语法	DirectoryString
示例	nsslapd-certmap-basedn: ou=People,dc=example,dc=com

2.1.61. nsslapd-close-on-failed-bind

如果 BIND 操作失败，请使用 nsslapd-close-on-failed-bind 配置属性来关闭来自服务器端的客户端连接。

启用此参数有助于减少目录服务器的负载，如果应用程序忽略 BIND 返回代码并继续发送请求。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-close-on-failed-bind: off

2.1.62. nsslapd-cn-uses-dn-syntax-in-dns

这个参数允许您在 CN 值中启用 DN。

目录服务器 DN 规范化程序遵循 RFC4514，并在 RDN 属性类型不基于 DN 语法时保留空格。但是 Directory 服务器的配置条目有时使用 cn 属性来存储 DN 值。例如，在 dn: cn="dc=A,dc=com", cn=mapping tree,cn=config 中，cn 应按照 DN 语法规范化。

如果需要此配置，请启用 nsslapd-cn-uses-dn-syntax-in-dns 参数。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-cn-uses-dn-syntax-in-dns: off

2.1.63. nsslapd-config

这个 **read-only** 属性是配置 **DN**。

参数	描述
条目 DN	cn=config
有效值	任何有效的配置 DN
默认值	
语法	DirectoryString
示例	nsslapd-config: cn=config

2.1.64. nsslapd-connection-buffer

此属性设置连接缓冲区行为。可能的值：

- **0: 禁用缓冲区。每次只读取单个协议数据单元(PDU)。**
- **1： 常规固定大小 LDAP_SOCKET_IO_BUFFER_SIZE 为 512 字节。**
- **2： 适应性缓冲区大小.**

如果客户端一次发送大量数据，则值 2 会提供更好的性能。例如，这适用于大型添加和修改操作，或者在复制过程中通过单一连接接收多个异步请求。

参数	描述
条目 DN	cn=config
有效值	0 | 1 | 2
默认值	1
语法	整数

参数	描述
示例	nsslapd-connection-buffer: 1

2.1.65. nsslapd-connection-nocanon

这个选项允许您启用或禁用 SASL NOCANON 标志。禁用 Directory 服务器避免了为出站连接查找 DNS 反向条目。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	on
语法	DirectoryString
示例	nsslapd-connection-nocanon: on

2.1.66. nsslapd-counters

nsslapd-counters 属性启用和禁用目录服务器数据库和服务器性能计数器。

通过跟踪更大的计数器，可能会有性能影响。为计数器关闭 64 位整数可降低性能，尽管对长期统计跟踪造成负面影响。

默认启用此参数。要禁用计数器，停止目录服务器，直接编辑 dse.ldif 文件，然后重新启动服务器。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	on
语法	DirectoryString

参数	描述
示例	nsslapd-counters: on

2.1.67. nsslapd-csnlogging

此属性设定是否要在访问日志中记录序列号(CSN)（如果可用）。默认情况下启用 CSN 日志记录。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	on
语法	DirectoryString
示例	nsslapd-csnlogging: on

2.1.68. nsslapd-defaultnamingcontext

此属性为所有配置的命名上下文提供命名上下文，客户端应默认使用这些命名上下文作为搜索基础。这个值作为 defaultNamingContext 属性复制到 root DSE，它允许客户端查询 root DSE 获取上下文，然后使用适当的基础启动搜索。

参数	描述
条目 DN	cn=config
有效值	任何 root 后缀 DN
默认值	默认用户后缀
语法	DN
示例	nsslapd-defaultnamingcontext: dc=example,dc=com

2.1.69. nsslapd-disk-monitoring

此属性可让线程每十(10)秒运行一次的线程，以检查磁盘上的可用磁盘空间或挂载到 Directory Server

数据库运行的挂载。如果可用磁盘空间低于配置的阈值，则服务器开始减少日志级别、禁用访问或审计日志，并删除轮转的日志。如果这没有足够的可用空间，则服务器将正常关闭（在 wanring 和 grace 期间之后）。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-disk-monitoring: on

2.1.70. nsslapd-disk-monitoring-grace-period

设置在服务器关闭前等待的宽限期，达到 第 2.1.73 节 “nsslapd-disk-monitoring-threshold” 中设置的磁盘空间限制的一半。这让管理员有时间来清理磁盘并防止关闭。

参数	描述
条目 DN	cn=config
有效值	任何整数（以分钟为单位的设置值）
默认值	60
语法	整数
示例	nsslapd-disk-monitoring-grace-period: 45

2.1.71. nsslapd-disk-monitoring-logging-critical

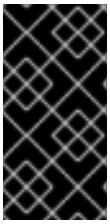
设定在日志目录通过磁盘空间限制 第 2.1.73 节 “nsslapd-disk-monitoring-threshold” 中设置的半向点时是否关闭服务器。

如果启用了，*则不会* 禁用日志记录，*也不会* 删除轮转日志，因为会减少服务器的磁盘用量。服务器只需进入关闭过程即可。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-disk-monitoring-logging-critical: on

2.1.72. nsslapd-disk-monitoring-readonly-on-threshold

如果可用磁盘空间达到 nsslapd-disk-monitoring-threshold 参数中设置的值的一半，则目录服务器会在 nsslapd-disk-monitoring-grace-period 中设置宽限期后关闭实例。但是，如果磁盘在实例停机前耗尽空间，数据可能会损坏。要防止这个问题，启用 nsslapd-disk-monitoring-readonly-on-threshold 参数，在达到阈值时目录服务器会将实例设置为只读模式。



重要

使用这个设置时，如果可用磁盘空间低于 nsslapd-disk-monitoring-threshold 中配置阈值的一半，则目录服务器不会启动。

必须重启该服务才能使此属性生效。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-disk-monitoring-readonly-on-threshold: off

2.1.73. nsslapd-disk-monitoring-threshold

设置阈值（以字节为单位）来评估服务器是否有足够可用磁盘空间。当空间达到这个阈值的一半后，

服务器就开始关闭过程。

例如，如果阈值是 2MB （默认），则当可用磁盘空间达到 1MB 后，服务器将开始关闭。

默认情况下，对目录服务器实例的配置、事务和数据库目录使用的磁盘空间评估阈值。如果启用了 第 2.1.71 节 “nsslapd-disk-monitoring-logging-critical” 属性，则日志目录包含在评估中。

参数	描述
条目 DN	cn=config
有效值	* 0 到最大 32 位整数值(2147483647)在 32 位系统中 * 0 到最大 64 位整数值(9223372036854775807)
默认值	2000000 (2MB)
语法	DirectoryString
示例	nsslapd-disk-monitoring-threshold: 2000000

2.1.74. nsslapd-dn-validate-strict

nsslapd-syntaxcheck 属性使服务器能够验证任何新的或修改的属性值是否与该属性所需的语法匹配。

但是，DN 的语法规则变得更为严格。试图在 RFC 4514 中强制执行 DN 语法规则可能会破坏许多使用旧语法定义的服务器。默认情况下，nsslapd-syntaxcheck 使用 RFC 1779 或 RFC 2253 验证 DN。

根据 RFC 4514 中的第 3 节，nsslapd-dn-validate-strict 属性明确为 DN 启用严格的语法验证。如果此属性设为 off （默认值），服务器会在检查该值以进行语法违反情况前对值进行规范化。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off

参数	描述
语法	DirectoryString
示例	nsslapd-dn-validate-strict: off

2.1.75. nsslapd-ds4-compatible-schema

使 cn=schema 中的 schema 与 4.x 版本的 Directory Server 兼容。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-ds4-compatible-schema: off

2.1.76. nsslapd-enable-turbo-mode

目录服务器 turbo 模式是一个功能，它允许 worker 线程专用于连接，并持续从该连接读取传入的操作。这可以在非常活跃的连接中提高性能，这个功能会被默认启用。

Worker 线程正在处理服务器接收的 LDAP 操作。在 nsslapd-threadnumber 参数中定义 worker 线程数量。每 5 秒，每个 worker 线程评估其当前连接的活动级别是否是所有已建立连接的最高级别之一。目录服务器将活动测量为自上一次检查以来启动的操作数量，如果当前连接的活动是最高状态，则以 turbo 模式切换 worker 线程。

如果您遇到长时间执行时间（日志文件中的etime 值）用于绑定操作（如一秒或更长时间），则停用 turbo 模式可能会提高性能。然而，在某些情况下，较长的绑定时间是网络或硬件问题的症状。在这些情况下，禁用 turbo 模式不会提高性能。

参数	描述
条目 DN	cn=config

参数	描述
有效值	on | off
默认值	on
语法	DirectoryString
示例	nsslapd-enable-turbo-mode: on

2.1.77. nsslapd-enable-upgrade-hash

在简单绑定过程中，Directory 服务器可能会因为绑定操作性质访问纯文本密码。如果启用了 nsslapd-enable-upgrade-hash 参数且用户身份验证，Directory 服务器会检查用户的 userPassword 属性是否使用 passwordStorageScheme 属性中设置的哈希算法。如果算法不同，服务器将使用 passwordStorageScheme 的算法哈希纯文本密码，并更新用户的 userPassword 属性的值。

例如，如果您导入了带有使用弱算法哈希的密码的用户条目，服务器会使用 passwordStorageScheme 中设置的算法自动重新哈希用户 上的密码，即 PBKDF2_SHA256。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	on
语法	DirectoryString
示例	nsslapd-enable-upgrade-hash: on

2.1.78. nsslapd-enquote-sup-oc

此属性已弃用，并将在以后的目录服务器版本中删除。

此属性控制 cn=schema 条目中包含的 objectclass 属性中的引用是否符合互联网草案 RFC 2252 指定的引用。默认情况下，Directory 服务器符合 RFC 2252，这表示不应用引号括起此值。在 上，只有非常旧的客户端需要将此值设置为，因此将其保留为 off。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-enquote-sup-oc: off

2.1.79. nsslapd-entryusn-global

nsslapd-entryusn-global 参数定义 USN 插件是否为所有后端数据库或单独为每个数据库分配唯一的更新序列号(USN)。对于所有后端数据库的唯一 USN，请在 上 将此参数设置为。

详情请查看 第 10.8 节 “entryusn”。

您不必重启服务器才能使此设置生效。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-entryusn-global: off

2.1.80. nsslapd-entryusn-import-initval

当条目从一个服务器导出并导入到另一个服务器时，条目更新序列号(USN)不会被保留，包括在初始化用于复制的数据库时。默认情况下，导入条目的条目 USNs 被设置为零。

可以使用 nsslapd-entryusn-import-initval 为条目 USNs 配置不同的初始值。这会设置一个起始 USN，用于所有导入的条目。

nsslapd-entryusn-import-initval 有两个可能的值：

- **一个整数，它是每个导入的条目使用的显式开始号。**
- ***接下来*，这意味着每个导入的条目都使用服务器的最高条目 USN 值，然后再导入操作，并递增一个。**

参数	描述
条目 DN	cn=config
有效值	任何整数 | 下一个
默认值	
语法	DirectoryString
示例	nsslapd-entryusn-import-initval: next

2.1.81. nsslapd-errorlog

此属性设置日志的路径和文件名，用于记录 Directory Server 生成的错误消息。这些消息可能会描述错误条件，但它们通常包含信息性条件，例如：

- **服务器启动和关闭时间.**
- **服务器使用的端口号。**

此日志包含不同的信息量，具体取决于 Log Level 属性的当前设置。请参阅 第 2.1.83 节 “nsslapd-errorlog-level” 了解更多信息。

参数	描述
条目 DN	cn=config

参数	描述
有效值	任何有效的文件名
默认值	/var/log/dirsrv/slapd-*instance*/errors
语法	DirectoryString
示例	nsslapd-errorlog: /var/log/dirsrv/slapd-*instance*/errors

要启用错误日志记录，此属性必须具有有效的路径和文件名，并且 nsslapd-errorlog-logging-enabled 配置属性必须在 上 切换到。表列出了这两个配置属性的四个可能值组合，以及它们的结果在禁用或启用错误日志方面的结果。

表 2.5. nsslapd-errorlog 配置属性可能的组合

dse.ldif 中的属性	值	启用或禁用日志记录
nsslapd-errorlog-logging-enabled nsslapd-errorlog	on 空字符串	Disabled
nsslapd-errorlog-logging-enabled nsslapd-errorlog	on *filename*	Enabled
nsslapd-errorlog-logging-enabled nsslapd-errorlog	off 空字符串	Disabled
nsslapd-errorlog-logging-enabled nsslapd-errorlog	off *filename*	Disabled

2.1.82. nsslapd-errorlog-compress

默认情况下，目录服务器不会压缩错误日志。将 nsslapd-errorlog-compress 设置为 on，以便在目录服务器轮转日志时启用错误日志压缩。

您不需要重新启动服务器以应用更改。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-errorlog-compress: on

2.1.83. nsslapd-errorlog-level

此属性设置目录服务器的日志记录级别。日志级别是可添加的；即，指定值 3 包括级别 1 和 2。

nsslapd-errorlog-level 的默认值为 16384。

您不必重启服务器才能使此设置生效。

参数	描述
条目 DN	cn=config
有效值	有关错误日志级别的完整列表，请参阅 错误日志记录级别。
默认值	16384
语法	整数
示例	nsslapd-errorlog-level: 8192

2.1.84. nsslapd-errorlog-list

此 read-only 属性提供错误日志文件列表。

参数	描述
条目 DN	cn=config
有效值	
默认值	无
语法	DirectoryString
示例	nsslapd-errorlog-list: errorlog2,errorlog3

2.1.85. nsslapd-errorlog-logexpirationtime

此属性设置日志文件在删除前允许达到的最长期限。此属性仅提供单元数量。单位（天、每周、月份等）由 nsslapd-errorlog-logexpirationtimeunit 属性提供。

参数	描述
条目 DN	cn=config
有效范围	-1 到最大 32 位整数值(2147483647) 值为 -1 或 0 表示日志永不过期。
默认值	-1
语法	整数
示例	nsslapd-errorlog-logexpirationtime: 1

2.1.86. nsslapd-errorlog-logexpirationtimeunit

此属性设置 nsslapd-errorlog-logexpirationtime 属性的单元。如果服务器未知单元，则日志永远不会过期。

参数	描述
条目 DN	cn=config
有效值	month | 周 | 天
默认值	month

参数	描述
语法	DirectoryString
示例	nsslapd-errorlog-logexpirationtimeunit: week

2.1.87. nsslapd-errorlog-logging-enabled

打开和关闭错误日志。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	on
语法	DirectoryString
示例	nsslapd-errorlog-logging-enabled: on

2.1.88. nsslapd-errorlog-logmaxdiskspace

此属性设置允许错误日志使用的最大磁盘空间量，以 MB 为单位。如果超过这个值，则会删除最旧的错误日志。

当设置最大磁盘空间时，请考虑可能会因为日志文件轮转而创建的日志文件总数。另外，请记住，目录服务器维护三个不同的日志文件（访问日志、审计日志和错误日志），每个日志文件消耗磁盘空间。将这些注意事项与错误日志的磁盘空间总量进行比较。

参数	描述
条目 DN	cn=config
有效范围	-1 | 1 到最大 32 位整数值(2147483647)，其中值为 -1 表示允许错误日志的磁盘空间的大小没有限制。
默认值	100
语法	整数

参数	描述
示例	nsslapd-errorlog-logmaxdiskspace: 10000

2.1.89. nsslapd-errorlog-logminfreediskspace

此属性以 MB 为单位设置允许的最小可用磁盘空间。当可用磁盘空间量低于此属性中指定的值时，将删除最旧的错误日志，直到释放足够的磁盘空间来满足此属性。

参数	描述
条目 DN	cn=config
有效范围	-1 (unlimited)| 1 到最大 32 位整数值(2147483647)
默认值	-1
语法	整数
示例	nsslapd-errorlog-logminfreediskspace: -1

2.1.90. nsslapd-errorlog-logrotationsync-enabled

此属性设定错误日志轮转是否与一天的特定时间同步。以这种方式同步日志轮转，可以在一天（例如每天午夜）的指定时间生成日志文件。这样可以更轻松地分析日志文件，因为它们然后直接映射到日历。

要使错误日志轮转与时间同步，必须使用 nsslapd-errorlog-logrotationsynchour 和 nsslapd-errorlog-logrotationsyncmin 属性值设置为轮转日志文件的时间和分钟。

例如，要每天在午夜轮转错误日志文件，请通过在 上 将其值设置为，然后将 nsslapd-errorlog-logrotationsynchour 和 nsslapd-errorlog-logrotationsyncmin 属性设为 0 来启用此属性。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off

参数	描述
语法	DirectoryString
示例	nsslapd-errorlog-logrotationsync-enabled: on

2.1.91. nsslapd-errorlog-logrotationsynchour

此属性设置轮转错误日志的一天小时。此属性必须与 nsslapd-errorlog-logrotationsync-enabled 和 nsslapd-errorlog-logrotationsyncmin 属性一起使用。

参数	描述
条目 DN	cn=config
有效范围	0 到 23
默认值	0
语法	整数
示例	nsslapd-errorlog-logrotationsynchour: 23

2.1.92. nsslapd-errorlog-logrotationsyncmin

此属性设置轮转错误日志的当天的分钟。此属性必须与 nsslapd-errorlog-logrotationsync-enabled 和 nsslapd-errorlog-logrotationsynchour 属性一起使用。

参数	描述
条目 DN	cn=config
有效范围	0 到 59
默认值	0
语法	整数
示例	nsslapd-errorlog-logrotationsyncmin: 30

2.1.93. nsslapd-errorlog-logrotationtime

此属性设置错误日志文件轮转之间的时间。此属性仅提供单元数量。单位（天、星期、月份等等）由 nsslapd-errorlog-logrotationtimeunit (Error Log Rotation Time Unit)属性提供。

目录服务器在配置的时间间隔到期后，在第一次写入操作时轮转日志，而不考虑日志的大小。

虽然不建议指定日志轮转的性能原因，但随着日志无限期增长，但可以通过两种方式指定此功能。将 nsslapd-errorlog-maxlogsperdir 属性值设置为 1，或者将 nsslapd-errorlog-logrotationtime 属性设置为 -1。服务器首先检查 nsslapd-errorlog-maxlogsperdir 属性，如果此属性值大于 1，则服务器会检查 nsslapd-errorlog-logrotationtime 属性。请参阅 第 2.1.96 节 “nsslapd-errorlog-maxlogsperdir” 了解更多信息。

参数	描述
条目 DN	cn=config
有效范围	-1 | 1 到最大 32 位整数值(2147483647)，其中值为 -1 表示错误日志文件轮转之间的时间没有限制。
默认值	1
语法	整数
示例	nsslapd-errorlog-logrotationtime: 100

2.1.94. nsslapd-errorlog-logrotationtimeunit

此属性设置 nsslapd-errorlog-logrotationtime (Error Log Rotation Time)的单元。如果服务器未知单元，则日志永远不会过期。

参数	描述
条目 DN	cn=config
有效值	month | week | day | hour | minute
默认值	week
语法	DirectoryString
示例	nsslapd-errorlog-logrotationtimeunit: day

2.1.95. nsslapd-errorlog-maxlogsize

此属性以 MB 为单位设置最大错误日志大小。当达到这个值时，错误日志会被轮转，服务器开始向新日志文件写入日志信息。如果 nsslapd-errorlog-maxlogsperdir 设置为 1，服务器会忽略此属性。

在设置最大日志大小时，请考虑可能会因为日志文件轮转而创建的日志文件总数。另外，请记住，Directory 服务器维护五个不同的日志文件（访问日志、审计日志、审计日志、错误日志、安全日志），每个日志文件消耗磁盘空间。将这些注意事项与错误日志的磁盘空间总量进行比较。

参数	描述
条目 DN	cn=config
有效范围	-1	1 到 32 位整数值(2147483647)，其中值为 -1 表示日志文件的大小没有限制。
默认值	100
语法	整数
示例	nsslapd-errorlog-maxlogsize: 100

2.1.96. nsslapd-errorlog-maxlogsperdir

此属性设置可包含在错误日志的目录中的错误日志总数。每次轮转错误日志时，都会创建一个新的日志文件。当错误日志目录中包含的文件数量超过此属性中存储的值时，会删除日志文件的最老版本。默认值为 1 日志。如果接受此默认值，服务器不会轮转日志，它会无限期地增长。

如果此属性的值大于 1，请检查 nsslapd-errorlog-logrotationtime 属性来建立是否指定了日志轮转。如果 nsslapd-errorlog-logrotationtime 属性的值为 -1，则没有日志轮转。请参阅 第 2.1.93 节 “nsslapd-errorlog-logrotationtime” 了解更多信息。

参数	描述
条目 DN	cn=config
有效范围	1 到最大 32 位整数值(2147483647)
默认值	1
语法	整数

参数	描述
示例	nsslapd-errorlog-maxlogsperdir: 10

2.1.97. nsslapd-errorlog-mode

此属性设置创建日志文件的访问模式或文件权限。有效值是 000 到 777 的组合，因为它们镜像编号或绝对 UNIX 文件权限。也就是说，该值必须是 3 位数字的组合，数字因 0 到 7 的不同而有所不同：

- 0 - None
- 1 - 只执行
- 2 - 仅写入
- 3 - 写入和执行
- 4 - 只读
- 5 - 读取和执行
- 6 - 读取和写入
- 7 - 读、写和执行

在 3 位数字中，第一个数字代表所有者的权限，第二个数字代表组的权限，第三个数字代表每个人的权限。更改默认值时，请记住 000 不允许访问日志，并且允许每个人的写入权限都可能导致日志被任何人覆盖或删除。

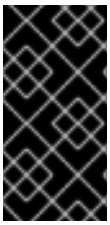
新配置的访问模式只会影响创建的新日志；当日志轮转到新文件时，会设置模式。

参数	描述
条目 DN	cn=config
有效范围	000 到 777
默认值	600
语法	整数
示例	nsslapd-errorlog-mode: 600

2.1.98. nsslapd-external-libs-debug-enabled

要在目录服务器中启用第三方日志记录，请使用 **nsslapd-external-libs-debug-enabled** 属性。

libldap 和 **libber** 等库会执行错误和调试日志，但这些记录在 **Directory Server** 日志中不可用。当 **nsslapd-external-libs-debug-enabled** 属性设置为 **on** 时，目录服务器可以使用 **libldap** 和 **libber** 软件包提供的所有日志级别。



重要

仅为调试目的启用 **nsslapd-external-libs-debug-enabled** 属性，因为它为所有操作生成详细的日志记录。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-external-libs-debug-enabled: off

2.1.99. nsslapd-force-sasl-external

在建立 **TLS** 连接时，客户端会首先发送其证书，然后使用 **SASL/EXTERNAL** 机制发出 **BIND** 请求。使用 **SASL/EXTERNAL** 告知目录服务器在 **TLS** 握手中使用证书中的凭证。但是，一些客户端在发送其

BIND 请求时不使用 SASL/EXTERNAL，因此目录服务器将绑定作为简单身份验证请求或匿名请求处理，并且 TLS 连接失败。

nsslapd-force-sasl-external 属性强制基于证书验证中的客户端使用 SASL/EXTERNAL 方法发送 BIND 请求。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	字符串
示例	nsslapd-force-sasl-external: on

2.1.100. nsslapd-groupevalnestlevel

此属性已弃用，在此处记录仅用于历史目的。

Access Control 插件不使用 nsslapd-groupevalnestlevel 属性指定的值来设置对组评估执行的嵌套级别数量。相反，嵌套的级别数量被硬编码为 5。

参数	描述
条目 DN	cn=config
有效范围	0 到 5
默认值	5
语法	整数
示例	nsslapd-groupevalnestlevel: 5

2.1.101. nsslapd-haproxy-trusted-ip

nsslapd-haproxy-trusted-ip 属性配置可信代理服务器列表。设置 nsslapd-haproxy-trusted-ip 时，目录服务器使用 HAProxy 协议通过额外的 TCP 标头接收客户端 IP 地址，以正确评估访问控制指令(ACI)

并记录客户端流量。

如果不受信任的代理服务器启动绑定请求，Directory 服务器会拒绝请求，并将以下信息记录到错误日志文件中：

```
[time_stamp] conn=5 op=-1 fd=64 Disconnect - Protocol error - Unknown Proxy - P4
```

参数	描述
条目 DN	cn=config
有效范围	IPv4 或 IPv6 地址
默认值	
语法	DirectoryString
示例	nsslapd-haproxy-trusted-ip: 127.0.0.1

2.1.102. nsslapd-idletimeout

此属性设置服务器关闭闲置 LDAP 客户端连接后的时间（以秒为单位）。0 表示服务器永远不会关闭闲置连接。此设置适用于所有连接和所有用户。当连接表被遍历时，会强制闲置超时，当 poll （） 不返回零时。因此，具有单一连接的服务器永远不会强制执行空闲超时。

使用 nsIdleTimeout 操作属性（可添加到用户条目中）来覆盖分配给此属性的值。

注意

对于具有数百万条目的大型数据库，此属性必须具有足够高的值，在线初始化过程可以完成或复制在与服务器超时时失败。或者，nsIdleTimeout 属性可以设置为用作供应商绑定 DN 的条目上的高值。

参数	描述
条目 DN	cn=config
有效范围	0 到最大 32 位整数值(2147483647)
默认值	3600

参数	描述
语法	整数
示例	nsslapd-idletimeout: 3600

2.1.103. nsslapd-ignore-virtual-attrs

此参数允许在搜索条目中禁用虚拟属性查找。

如果不需要虚拟属性，您可以在搜索结果中禁用虚拟属性查找来提高搜索速度。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	on
语法	DirectoryString
示例	nsslapd-ignore-virtual-attrs: on

2.1.104. nsslapd-instancedir

此属性已弃用。现在，有单独的配置参数用于特定于实例的路径，如 nsslapd-certdir 和 nsslapd-lockdir。有关所设置的特定目录路径，请参阅文档。

2.1.105. nsslapd-ioblocktimeout

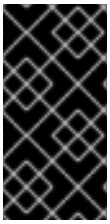
此属性设置与停滞 LDAP 客户端关闭后的时间（以毫秒为单位）。当 LDAP 客户端没有为读或写操作进行任何 I/O 处理时，它被视为已停止工作。

参数	描述
条目 DN	cn=config
有效范围	0 到最大 32 位整数值(2147483647) in ticks

参数	描述
默认值	10000
语法	整数
示例	nsslapd-ioblocktimeout: 10000

2.1.106. nsslapd-lastmod

此属性设置 Directory 服务器是否为新创建或更新的条目维护 creatorsName,createTimestamp,modifiersName, 和 modifyTimestamp 操作属性。



重要

红帽建议不要禁用跟踪这些属性。如果禁用，条目不会获得 nsUniqueID 属性中分配的唯一 ID，复制不起作用。

您不必重启服务器才能使此设置生效。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	on
语法	DirectoryString
示例	nsslapd-lastmod: on

2.1.107. nsslapd-ldapiautobind

nsslapd-ldapiautobind 设置服务器是否允许用户使用 LDAPI 自动绑定到目录服务器。Autobind 将系统用户的 UID 或 GUID 号映射到目录服务器用户，并根据这些凭证自动将用户验证到目录服务器。目录服务器连接通过 UNIX 套接字进行。

除了启用自动绑定外，配置 autobind 需要配置映射条目。nsslapd-ldapimaprootdn 将系统上的 root

用户映射到 Directory Manager。nsslapd-ldapimaptoentries 将常规用户映射到目录服务器用户，具体取决于 nsslapd-ldapiuidnumbertype,nsslapd-ldapigidnumbertype, 和 nsslapd-ldapientrysearchbase 属性中定义的参数。

只有启用了 LDAPI 时，才可启用 Autobind，即 nsslapd-ldapilisten 并且 nsslapd-ldapifilepath 属性设置为 LDAPI 套接字。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-ldapiautobind: off

2.1.108. nsslapd-ldapientrysearchbase

通过自动绑定，可以根据系统用户的 UID 和 GUID 号将系统用户映射到目录服务器用户条目。这需要为 UID 号(nsslapd-ldapiuidnumbertype)和 GUID 号(nsslapd-ldapigidnumbertype)设置 Directory Server 参数，并设置搜索基础，用于搜索匹配的用户条目。

nsslapd-ldapientrysearchbase 提供子树来搜索用于 autobind 的用户条目。

参数	描述
条目 DN	cn=config
有效值	DN
默认值	创建服务器实例时创建的后缀，如 **dc=example,dc=com**
语法	DN
示例	nsslapd-ldapientrysearchbase: ou=people,dc=example,dc=om

2.1.109. nsslapd-ldapifilepath

LDAPI 通过 UNIX 套接字而不是 TCP 将用户连接到 LDAP 服务器。为了配置 LDAPI，服务器必须配置为通过 UNIX 套接字进行通信。要使用的 UNIX 套接字在 nsslapd-ldapifilepath 属性中设置。

参数	描述
条目 DN	cn=config
有效值	任何目录路径
默认值	/var/run/dirsrv/slapd-example.socket
语法	case-exact 字符串
示例	nsslapd-ldapifilepath: /var/run/slapd-example.socket

2.1.110. nsslapd-ldapigidnumbertype

Autobind 可用于系统用户自动向服务器验证服务器，并使用 UNIX 套接字连接到服务器。要将系统用户映射到目录服务器用户进行身份验证，系统用户的 UID 和 GUID 号应映射到目录服务器属性。nsslapd-ldapigidnumbertype 属性指向 Directory Server 属性，将系统 GUID 映射到用户条目。

如果启用了 LDAPI (nsslapd-ldapilisten 和 nsslapd-ldapifilepath)、autobind 被启用(nsslapd-ldapiautobind)，并且为常规用户启用了 autobind 映射(nsslapd-ldapimaptoentries)，并且为常规用户启用了 autobind 映射(nsslapd-ldapimaptoentries)。

参数	描述
条目 DN	cn=config
有效值	任何目录服务器属性
默认值	gidNumber
语法	DirectoryString
示例	nsslapd-ldapigidnumbertype: gidNumber

2.1.111. nsslapd-ldapilisten

nsslapd-ldapilisten 启用 LDAPI 连接到目录服务器。LDAPI 允许用户通过 UNIX 套接字而不是标准 TCP 端口连接到目录服务器。除了通过将 nsslapd-ldapilisten 设置为 on 来启用 LDAPI 外，nsslapd-

ldapifilepath 属性中还必须为 LDAPI 设置 UNIX 套接字。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	on
语法	DirectoryString
示例	nsslapd-ldapilisten: on

2.1.112. nsslapd-ldapimaprootdn

nsslapd-ldapimaprootdn 属性已弃用。使用 nsslapd-rootdn 参数将系统根条目映射到 root DN 条目。

使用 autobind 时，系统用户映射到目录服务器用户，然后通过 UNIX 套接字自动向目录服务器进行身份验证。

root 系统用户(UID 为 0 的用户)映射到 nsslapd-ldapimaprootdn 属性中指定的任何目录服务器条目。

参数	描述
条目 DN	cn=config
有效值	任何 DN
默认值	cn=Directory Manager
语法	DN
示例	nsslapd-ldapimaprootdn: cn=Directory Manager

2.1.113. nsslapd-ldapimaptoentries

使用 autobind 时，系统用户映射到目录服务器用户，然后通过 UNIX 套接字自动向目录服务器进行身份验证。这个映射对 root 用户自动进行，但必须通过 nsslapd-ldapimaptoentries 属性为常规系统用户

启用它。将此属性设置为 on，为常规系统用户启用到目录服务器条目的映射。如果没有启用此属性，则只有 root 用户可以使用 autobind 对目录服务器进行身份验证，所有其他用户则匿名连接。

映射本身通过 nsslapd-ldapiuidnumbertype 和 nsslapd-ldapigidnumbertype 属性进行配置，这会将目录服务器属性映射到用户的 UID 和 GUID 号。

如果启用了 LDAPI (nsslapd-ldapilisten 和 nsslapd-ldapifilepath)，并且启用了 autobind (nsslapd-ldapiautobind)，用户只能连接到具有 autobind 的服务器。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-ldapimaptoentries: on

2.1.114. nsslapd-ldapiuidnumbertype

Autobind 可用于系统用户自动向服务器验证服务器，并使用 UNIX 套接字连接到服务器。要将系统用户映射到目录服务器用户进行身份验证，系统用户的 UID 和 GUID 号必须映射到目录服务器属性。nsslapd-ldapiuidnumbertype 属性指向 Directory Server 属性，将系统 UID 映射到用户条目。

如果启用了 LDAPI (nsslapd-ldapilisten 和 nsslapd-ldapifilepath)、autobind 被启用(nsslapd-ldapiautobind)，并且为常规用户启用了 autobind 映射(nsslapd-ldapimaptoentries)，并且为常规用户启用了 autobind 映射(nsslapd-ldapimaptoentries)。

参数	描述
条目 DN	cn=config
有效值	任何目录服务器属性
默认值	uidNumber
语法	DirectoryString

参数	描述
示例	nsslapd-ldapiuidnumbertype: uidNumber

2.1.115. nsslapd-ldifdir

在使用 db2ldif 或 db2ldif.pl 时，目录服务器以 LDAP 数据交换格式(LDIF)格式将文件导出到此参数中设置的目录。该目录必须由 Directory Server 用户和组所有。只有此用户和组必须在这个目录中具有读写访问权限。

必须重启该服务才能使此属性生效。

参数	描述
条目 DN	cn=config
有效值	Directory 服务器用户可写入的任何目录
默认值	/var/lib/dirsrv/slapd-*instance_name*/ldif/
语法	DirectoryString
示例	nsslapd-ldifdir: /var/lib/dirsrv/slapd-*instance_name*/ldif/

2.1.116. nsslapd-listen-backlog-size

此属性设置套接字连接 backlog 的最大值。侦听服务设定可用于接收进入的连接的套接字的数量。backlog 设置设置套接字队列(sockfd)在拒绝连接前可以增长的最大长度。

参数	描述
条目 DN	cn=config
有效值	最大 64 位整数值(9223372036854775807)
默认值	128
语法	整数
示例	nsslapd-listen-backlog-size: 128

2.1.117. nsslapd-listenhost

此属性允许多个目录服务器实例在多主目录计算机上运行（或者，可以限制侦听多主目录计算机的一个接口）。可能存在多个与单个hos tname 关联的 IP 地址，这些 IP 地址可以是 IPv4 和 IPv6 的组合。这个参数可用于将 Directory 服务器实例限制为单个 IP 接口。

如果为主机名提供 nsslapd-listenhost 值，则目录服务器会响应与主机名关联的每个接口的请求。如果给出一个 IP 接口(IPv4 或 IPv6)作为 nsslapd-listenhost 值，目录服务器只响应发送到该特定接口的请求。可以使用 IPv4 或 IPv6 地址。

必须重启服务器才能使此属性生效。

参数	描述
条目 DN	cn=config
有效值	任何本地主机名、IPv4 或 IPv6 地址
默认值	
语法	DirectoryString
示例	nsslapd-listenhost: ldap.example.com

2.1.118. nsslapd-localhost

此属性指定目录服务器在其上运行的主机机器。此属性创建组成 MMR 协议一部分的引用 URL。在带有故障转移节点的高可用性配置中，引用应指向集群的虚拟名称，而不是本地主机名。

参数	描述
条目 DN	cn=config
有效值	任何完全限定主机名。
默认值	安装的机器的主机名。
语法	DirectoryString
示例	nsslapd-localhost: phonebook.example.com

2.1.119. nsslapd-localssf

nsslapd-localssf 参数为 LDAPI 连接设置安全强度因子(SSF)。只有 nsslapd-localssf 中设置的值大于或等于 nsslapd-minssf 参数中设置的值时，目录服务器才允许 LDAPI 连接。因此，LDAPI 连接满足 nsslapd-minssf 中设置的最小 SSF。

您不必重启服务器才能使此设置生效。

参数	描述
条目 DN	cn=config
有效值	0 到最大 32 位整数值(2147483647)
默认值	71
语法	整数
示例	nsslapd-localssf: 71

2.1.120. nsslapd-localuser

此属性将用户设置为目录服务器运行。用户运行的组派生自此属性的组，方法是检查用户的主组。如果用户更改，那么此实例的所有特定文件和目录都需要使用 chown 等工具更改为由新用户所有。

在配置服务器实例时，首先设置 nsslapd-localuser 的值。

参数	描述
条目 DN	cn=config
有效值	任何有效的用户
默认值	
语法	DirectoryString
示例	nsslapd-localuser: dirsrv

2.1.121. nsslapd-lockdir

这是服务器用于锁定文件的目录的完整路径。默认值为 /var/lock/dirsrv/slapd-*实例*。对这个值的更改不会生效，直到服务器重启为止。

参数	描述
条目 DN	cn=config
有效值	由服务器用户 ID 拥有的目录的绝对路径，其对服务器 ID 具有写入访问权限
默认值	/var/lock/dirsrv/slapd-*instance*
语法	DirectoryString
示例	nsslapd-lockdir: /var/lock/dirsrv/slapd-*instance*

2.1.122. nsslapd-logging-hr-timestamps-enabled

控制日志是否使用高分辨率时间戳和纳秒精度，或使用带有一秒精度的标准解析时间戳。默认启用此选项。将这个选项设置为 **off**，将日志时间戳恢复为一秒精度。

此设置不需要重启服务器才能生效。

参数	描述
条目 DN	cn=config
有效值	**on** | **off**
默认值	**on**
语法	DirectoryString
示例	nsslapd-logging-hr-timestamps-enabled: on

2.1.123. nsslapd-malloc-mmap-threshold

如果使用 **systemctl** 实用程序将目录服务器实例作为服务启动，则环境变量不会传递给服务器，除非您在 **/etc/sysconfig/dirsrv -*instance_name*** 文件中设置它们。详情请查看 **systemd.exec(3) man page**。

nsslapd-malloc-mmap-threshold 参数可让您在 Directory Server 配置中设置值，而不是手动编辑服务文件来设置 M_MMAP_THRESHOLD 环境变量。详情请查看 mallopt(3)手册页中的 M_MMAP_THRESHOLD 参数描述。

此设置不需要重启服务器才能生效。

参数	描述
条目 DN	cn=config
有效范围	0 - 33554432
默认值	请参阅 **mallopt**(3)手册页中的 **M_MMAP_THRESHOLD** 参数描述。
语法	整数
示例	nsslapd-malloc-mmap-threshold: 33554432

2.1.124. nsslapd-malloc-mxfast

如果使用 systemctl 实用程序将目录服务器实例作为服务启动，则环境变量不会传递给服务器，除非您在 /etc/sysconfig/dirsrv -*instance_name* 文件中设置它们。详情请查看 systemd.exec(3) man page。

nsslapd-malloc-mxfast 参数允许您设置目录服务器配置中的值，而不是手动编辑服务文件来设置 M_MXFAST 环境变量。详情请查看 mallopt(3) man page 中的 M_MXFAST 参数描述。

此设置不需要重启服务器才能生效。

参数	描述
条目 DN	cn=config
有效范围	0 - 80 * (sizeof(size_t) / 4)
默认值	请参阅 **mallopt**(3) man page 中的**M_MXFAST** 参数描述。
语法	整数

参数	描述
示例	nsslapd-malloc-mxfast: 1048560

2.1.125. nsslapd-malloc-trim-threshold

如果使用 systemctl 实用程序将目录服务器实例作为服务启动，则环境变量不会传递给服务器，除非您在 /etc/sysconfig/dirsrv -*instance_name* 文件中设置它们。详情请查看 systemd.exec(3) man page。

nsslapd-malloc-trim-threshold 参数可让您在 Directory Server 配置中设置值，而不是手动编辑服务文件来设置 M_TRIM_THRESHOLD 环境变量。详情请查看 mallopt(3) man page 中的 M_TRIM_THRESHOLD 参数描述。

此设置不需要重启服务器才能生效。

参数	描述
条目 DN	cn=config
有效范围	0 到 2^31-1
默认值	请参阅 **mallopt**(3)手册页中的 **M_TRIM_THRESHOLD** 参数描述。
语法	整数
示例	nsslapd-malloc-trim-threshold: 131072

2.1.126. nsslapd-maxbersize

定义传入消息允许的最大大小（以字节为单位）。这限制了目录服务器可处理的 LDAP 请求大小。限制请求大小可防止某种形式拒绝服务攻击。

限制适用于 LDAP 请求的总大小。例如，如果请求要添加条目，并且请求中的条目大于配置的值或默认值，则拒绝添加请求。但是，这个限制不适用于复制进程。在更改此属性前请小心。

此设置不需要重启服务器才能生效。

参数	描述
条目 DN	cn=config
有效范围	0 - 2GB (2,147,483,647 字节) 零 **0** 表示应使用默认值。
默认值	2097152
语法	整数
示例	nsslapd-maxbersize: 2097152

2.1.127. nsslapd-maxdescriptors

nsslapd-maxdescriptors 属性设置目录服务器可以使用的最大平台依赖文件描述符数。当客户端连接到服务器以及某些服务器活动（如索引维护）时，都会使用文件描述符。文件描述符也供日志文件、数据库文件（索引和事务日志）使用，作为到其他服务器的套接字，以进行复制和链的传出连接。

用于 TCP/IP 用于服务客户端连接的描述符数量等于 nsslapd-maxdescriptors 属性减去 nsslapd-reservedescriptors 属性决定的非客户端连接的文件描述符数量。如需了解更多详细信息，请参阅 nsslapd-reservedescriptors。

您为 nsslapd-maxdescriptors 属性设置的数量不能大于操作系统允许 ns-slapd 进程使用的文件描述符总数。这个数字因操作系统而异。有关文件描述符限制和配置的详情，请查看操作系统文档。您可以使用 dsktune 程序建议对系统内核或 TCP/IP 调优属性的更改。

如果您设置了 nsslapd-maxdescriptors 属性的值过高，Directory 服务器会查询操作系统以获得最大允许值，然后使用这个值。目录服务器也会在错误日志中发出警告。如果您使用 ldapmodify 远程设置无效的值，服务器会拒绝新值，保留旧值，并返回错误。

如果 Directory 服务器拒绝连接，请增加 nsslapd-maxdescriptors 属性值，因为它没有文件描述符，并将以下信息写入 Directory Server 错误日志文件中：

> **Not listening for new connections -- too many fds open**

注意

UNIX shell 通常对文件描述符数量有可配置的限制。有关 限制和 ulimit 的更多信息，请参阅操作系统文档，因为这些限制通常会导致问题。

您必须重启服务器以应用更改。

参数	描述
条目 DN	cn=config
有效范围	依赖操作系统
默认值	1048576.服务器在其上运行的操作系统的文件描述符限制
语法	整数
示例	nsslapd-maxdescriptors: 64000

2.1.128. nsslapd-maxsasliosize

当用户通过 SASL GSS-API 向目录服务器进行身份验证时，服务器必须为客户端分配一定数量的内存来执行 LDAP 操作，具体取决于客户端请求的内存量。攻击者可能会发送此类大型数据包大小，它会使目录服务器崩溃或将其无限绑定，作为拒绝服务攻击的一部分。

使用 nsslapd-maxsasliosize 属性可以限制目录服务器允许 SASL 客户端的数据包大小。此属性设置服务器将接受的最大允许 SASL IO 数据包大小。

当传入的 SASL IO 数据包大于 nsslapd-maxsasliosize 限制时，服务器会立即断开客户端，并将信息记录到错误日志中，以便管理员根据需要调整设置。

此属性值以字节为单位指定。

参数	描述
条目 DN	cn=config

参数	描述
有效范围	* -1 （无限）到最大 32 位整数值(2147483647) * -1 (unlimited)到 64 位系统上最大 64 位整数值(9223372036854775807)
默认值	2097152 (2MB)
语法	整数
示例	nsslapd-maxsasliosize: 2097152

2.1.129. nsslapd-maxthreadsperconn

定义连接应使用的最大线程数。对于客户端绑定的正常操作，且仅在未绑定前执行一个或多个操作，请使用默认值。对于客户端绑定和同时发出多个请求的情况，请增加这个值以允许每个连接有足够的资源来执行所有操作。此属性无法从服务器控制台获得。

参数	描述
条目 DN	cn=config
有效范围	1 到最大 threadnumber
默认值	5
语法	整数
示例	nsslapd-maxthreadsperconn: 5

2.1.130. nsslapd-minssf

安全强度因素是 根据连接关键强度的相对衡量方式。SSF 决定 TLS 或 SASL 连接的安全程度。nsslapd-minssf 属性为服务器的任何连接设置最小 SSF 要求；任何比最小 SSF 更弱的连接尝试都会被拒绝。

TLS 和 SASL 连接可以在与目录服务器的连接中混合使用。这些连接通常具有不同的 SSF。两个 SSF 的更高用于与最低 SSF 要求进行比较。

将 SSF 值设置为 0 表示没有最小设置。

参数	描述
条目 DN	cn=config
有效值	任何正整数
默认值	0 (off)
语法	DirectoryString
示例	nsslapd-minssf: 128

2.1.131. nsslapd-minssf-exclude-rootdse

安全强度因素是 根据连接关键强度的相对衡量方式。SSF 决定 TLS 或 SASL 连接的安全程度。

nsslapd-minssf-exclude-rootdse 属性为任何与服务器的连接设置最小 SSF 要求，*除了查询 root DSE*。这对大多数连接强制实施适当的 SSF 值，同时仍然允许客户端从 root DSE 获取服务器配置所需的信息，而无需首先建立安全连接。

参数	描述
条目 DN	cn=config
有效值	任何正整数
默认值	0 (off)
语法	DirectoryString
示例	nsslapd-minssf-exclude-rootdse: 128

2.1.132. nsslapd-moddn-aci

此参数控制 ACI 检查目录条目何时从一个子树移到另一个子树，并在 moddn 操作中使用源和目标限制。为了向后兼容，您可以禁用 ACI 检查。

参数	描述
条目 DN	cn=config

参数	描述
有效值	on | off
默认值	on
语法	DirectoryString
示例	nsslapd-moddn-aci: on

2.1.133. nsslapd-nagle

当此属性的值为 off 时，会设置 TCP_NODELAY 选项，以便 LDAP 响应（如条目或结果消息）立即发送到客户端。当属性打开时，会应用默认的 TCP 行为；特别是，发送数据会延迟，以便可将额外的数据分组到底层网络 MTU 大小的一个数据包中，通常为以太网的 1500 字节。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-nagle: off

2.1.134. nsslapd-ndn-cache-enabled

规范化可区分名称(DN)是一个资源密集型任务。如果启用了 nsslapd-ndn-cache-enabled 参数，Directory 服务器会在内存中缓存规范化 DN。更新 nsslapd-ndn-cache-max-size 参数，以设置此缓存的最大大小。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	on
语法	DirectoryString

参数	描述
示例	nsslapd-ndn-cache-enabled: on

2.1.135. nsslapd-ndn-cache-max-size

规范化可区分名称(DN)是一个资源密集型任务。如果启用了 **nsslapd-ndn-cache-enabled** 参数，Directory 服务器会在内存中缓存规范化 DN。**nsslapd-ndn-cache-max-size** 参数设置此缓存的最大大小。

如果请求的 DN 尚未缓存，它将被规范化并添加。当超过缓存大小限制时，目录服务器会从缓存中删除最近使用的 10,000 DN。但是，至少 10,000 个 DN 会被缓存。

参数	描述
条目 DN	cn=config
有效值	0 到最大 32 位整数值(2147483647)
默认值	20971520
语法	整数
示例	nsslapd-ndn-cache-max-size: 20971520

2.1.136. nsslapd-outbound-ldap-io-timeout

此属性限制所有出站 LDAP 连接的 I/O 等待时间。默认值为 **300000** 毫秒(5 分钟)。值 **0** 表示服务器不会对 I/O 等待时间施加限制。

参数	描述
条目 DN	cn=config
有效范围	0 到最大 32 位整数值(2147483647)
默认值	300000
语法	DirectoryString

参数	描述
示例	nsslapd-outbound-ldap-io-timeout: 300000

2.1.137. nsslapd-pagedsizelimit

此属性设置从搜索操作返回的最大条目数，*特别是使用简单页面的结果控制*。这会覆盖 **paged** 搜索的 **nsslapd-sizelimit** 属性。

如果这个值为零，则使用 **nsslapd-sizelimit** 属性进行分页搜索和非页搜索。

参数	描述
条目 DN	cn=config
有效范围	-1 到最大 32 位整数值(2147483647)
默认值	
语法	整数
示例	nsslapd-pagedsizelimit: 10000

2.1.138. nsslapd-plug-in

此只读属性列出了插件条目的 **DN**，用于服务器加载的语法和匹配的规则插件。

2.1.139. nsslapd-plugin-binddn-tracking

将用于操作的绑定 **DN** 设置为条目的修饰符，即使操作本身是由服务器插件启动的。执行操作的特定插件列在单独的操作属性 **internalModifiersname** 中。

一个更改可以触发目录树中的其他自动更改。例如，当删除用户时，该用户会自动从其所属的任何组中删除，这些组通过引用完整性插件自动移除。用户的初始删除由与服务器绑定的任何用户帐户执行，但对组（默认）的更新显示为由插件执行的，不显示有关哪个用户启动该更新的信息。**nsslapd-plugin-binddn-tracking** 属性允许服务器跟踪哪个用户源自更新操作，以及实际执行它的内部插件。例如：

```
dn: cn=my_group,ou=groups,dc=example,dc=com
modifiersname: uid=jsmith,ou=people,dc=example,dc=com
internalModifiersname: cn=referential integrity plugin,cn=plugins,cn=config
```

此属性默认为禁用。

参数	描述
条目 DN	cn=config
有效范围	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-plugin-binddn-tracking: on

2.1.140. nsslapd-plugin-logging

默认情况下，即使将访问日志记录设置为记录内部操作，插件内部操作也不会记录在访问日志文件中。您可以使用此参数在全局范围内启用日志记录，而不是在每个插件配置中启用日志记录。

启用后，插件会使用此全局设置，并在启用时记录访问和审计事件。

如果启用了 nsslapd-plugin-logging，并且 nsslapd-accesslog-level 设置为记录内部操作，未索引的搜索和其他内部操作会记录到访问日志文件中。

如果没有设置 nsslapd-plugin-logging，则插件中的未索引搜索仍然记录在 Directory Server 错误日志中。

参数	描述
条目 DN	cn=config
有效范围	on | off
默认值	off
语法	DirectoryString

参数	描述
示例	nsslapd-plugin-logging: off

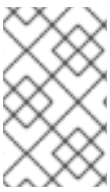
2.1.141. nsslapd-port

此属性提供用于标准 LDAP 通信的 TCP/IP 端口号。要通过此端口运行 TLS，请使用 Start TLS 扩展操作。这个所选端口在主机系统中必须是唯一的；确保其他应用程序不会尝试使用相同的端口号。指定小于 1024 的端口号表示目录服务器必须以 root 用户身份启动。

服务器在启动时将其 uid 设置为 nsslapd-localuser 值。在更改配置目录的端口号时，必须更新配置目录中对应的服务器实例条目。

必须重新启动服务器，才能考虑端口号更改。

参数	描述
条目 DN	cn=config
有效范围	0 到 65535
默认值	389
语法	整数
示例	nsslapd-port: 389



注意

如果启用了 LDAPS 端口，将端口号设为0以禁用 LDAP 端口。

2.1.142. nsslapd-privatenamespaces

此 read-only 属性包含私有命名上下文 cn=config、cn=schema 和 cn=monitor 的列表。

参数	描述
条目 DN	cn=config

参数	描述
有效值	cn=config, cn=schema, 和 cn=monitor
默认值	
语法	DirectoryString
示例	nsslapd-privatenamespaces: cn=config

2.1.143. nsslapd-pwpolicy-inherit-global

如果没有设置精细的密码语法，即使配置了全局密码语法，也不会检查新的或更新的密码。要继承全局细粒度密码语法，请在 上 将此属性设置为。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-pwpolicy-inherit-global: off

2.1.144. nsslapd-pwpolicy-local

打开和关闭细粒度(subtree- 和用户级)密码策略。

如果此属性的值为 off，则目录中所有条目(cn=Directory Manager除外)都受到全局密码策略的影响；服务器会忽略任何定义的子树/用户级别密码策略。

如果此属性在 上具有，则服务器会在子树和用户级别检查密码策略并强制实施这些策略。

参数	描述
条目 DN	cn=config

参数	描述
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-pwpolicy-local: off

2.1.145. nsslapd-readonly

此属性设置整个服务器是否处于只读模式，这意味着不可修改数据库或配置信息中的数据。任何尝试以只读模式修改数据库会返回一个错误，表示服务器不会执行该操作。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-readonly: off

2.1.146. nsslapd-referral

这个多值属性指定当服务器接收不属于本地树的条目请求时，后缀返回的 LDAP URL。也就是说，后缀与任何后缀属性上指定的值不匹配。例如，假设服务器仅包含条目：

> ou=People,dc=example,dc=com

但是请求用于此条目：

> ou=Groups,dc=example,dc=com

在这种情况下，引用将传递回客户端，以便 LDAP 客户端找到包含请求条目的服务器。虽然每个目录服务器实例只允许一个引用，但这个引用可以有多个值。

注意

要使用 TLS 通信，引用属性应采用 ldaps://*server-location* 的形式。

启动 **TLS 不支持引用。**

参数	描述
条目 DN	cn=config
有效值	任何有效的 LDAP URL
默认值	
语法	DirectoryString
示例	nsslapd-referral: ldap://ldap.example.com/dc=example,dc=com

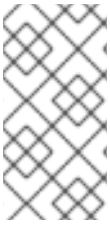
2.1.147. nsslapd-referralmode

设置后，此属性会返回任何后缀上任何请求的引用。

参数	描述
条目 DN	cn=config
有效值	任何有效的 LDAP URL
默认值	
语法	DirectoryString
示例	nsslapd-referralmode: ldap://ldap.example.com

2.1.148. nsslapd-require-secure-binds

这个参数要求用户通过 TLS、StartTLS 或 SASL 等受保护的连接验证目录，而不是常规连接。



注意

这只适用于经过身份验证的绑定。匿名绑定和未经身份验证的绑定仍可通过标准频道完成，即使启用了 nsslapd-require-secure-binds。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-require-secure-binds: on

2.1.149. nsslapd-requiresrestart

此参数列出在修改后需要重启服务器的其他核心配置属性。这意味着，如果 nsslapd-requiresrestart 中列出的任何属性已更改，则新设置在服务器重启后不会生效。属性列表可在 ldapsearch 中返回：

```
ldapsearch -D "cn=Directory Manager" -W -p 389 -h server.example.com -b "cn=config" -s sub -x "(objectclass=*)" | grep nsslapd-requiresrestart
```

此属性是多值。

参数	描述
条目 DN	cn=config
有效值	任何核心服务器配置属性
默认值	
语法	DirectoryString
示例	nsslapd-requiresrestart: nsslapd-cachesize

2.1.150. nsslapd-reservedescriptors

nsslapd-reservedescriptors 属性指定目录服务器为管理非客户端连接而保留的文件描述符数量，如索引管理和管理复制。

您不需要为大多数目录服务器安装更改 nsslapd-reservedescriptors 属性值。但是，如果以下所有都为 true，请考虑在此属性上增加值：

- 服务器复制到大量消费者服务器（超过 10 个），或者服务器维护大量索引文件（超过 30 个）。
- 服务器服务了大量 LDAP 连接。
- 错误消息报告服务器无法打开文件描述符（实际错误消息因服务器尝试执行的操作而异，但这些错误消息与管理客户端 LDAP 连接 *无关*。

如果您增大此属性的值，则更多 LDAP 客户端可能无法访问该目录。除了增加 nsslapd-reservedescriptors 值外，还必须增加 nsslapd-maxdescriptors 属性的值。如果服务器已使用操作系统允许进程使用的最大文件描述符数，则可能无法增加 nsslapd-maxdescriptors 值。如果出现这种情况，则通过导致 LDAP 客户端搜索替代目录副本来减少服务器上的负载。详情请查看操作系统文档和 nsslapd-maxdescriptors 属性描述。

要协助计算为 nsslapd-reservedescriptors 属性设置的文件描述符数量，请使用以下公式：

```
nsslapd-reservedescriptor = 20 + (pass:quotes[NldbmBackends] * 4) +
pass:quotes[NglobalIndex] +
pass:quotes[ReplicationDescriptor] + pass:quotes[ChainingBackendDescriptors] +
pass:quotes[PTADescriptors] + pass:quotes[SSLDescriptors]
```

- *NldbmBackends* 是 ldbm 数据库的数量。
- *NglobalIndex* 是所有数据库配置的索引的总数，包括系统索引。（默认为 8 个系统索引和每个数据库 17 个额外的索引）。
- *复制描述符* 是 8 (8)，以及服务器中可以充当供应商或中心的副本数(*NSupplierReplica*)。
- *ChainingBackendDescriptors* 是 *NchainingBackend* times the *nsOperationConnectionsLimit*（一个 chaining 或 database link configuration 属性，默认

为 10 ）。

- 如果尚未配置 PTA，则 *PTADescriptors* 为 3 ；如果尚未配置 PTA，则 PTADescriptors 为 0。

- 如果配置了 TLS，则 *SSLDescriptors* 为 5 (4 文件 + 1 listensocket)，如果未配置 TLS，则为 0。

重新启动服务器以应用更改。

参数	描述
条目 DN	cn=config
有效范围	1 到 65535
默认值	64
语法	整数
示例	nsslapd-reservedescriptors: 64

2.1.151. nsslapd-return-exact-case

返回客户端请求的属性类型名称的确切情况。虽然 LDAPv3 兼容客户端必须忽略属性名称的情况，但有些客户端应用程序需要属性名称来完全匹配属性的大小，因为它在 Directory Server 返回属性时列在 schema 中，作为搜索或修改操作的结果。但是，大多数客户端应用程序会忽略属性的情况；因此，默认情况下，此属性被禁用。不要修改它，除非有传统客户端可以检查从服务器返回的属性名称时。

必须重启服务器才能使此属性生效。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	on

参数	描述
语法	DirectoryString
示例	nsslapd-return-exact-case: off

2.1.152. nsslapd-return-original-entrydn

使用 nsslapd-return-original-entrydn 参数来管理目录服务器在搜索操作期间如何将可分辨名称(DN)返回给客户端应用程序。

当在 上将 nsslapd-return-original-entrydn 参数设置为 时，目录服务器通过获取操作属性 dsEntryDN 的值来返回它最初添加到数据库中的方式。因此，如果您添加或修改了条目 uid=User,ou=PEople,dc=ExaMPlE,DC=COM, Directory Server 返回相同的 DN uid=User,ou=PEople,dc=ExaMPlE,DC=COM。

当 nsslapd-return-original-entrydn 参数设置为 off 时，目录服务器会通过将条目和基本 DN 的 Relative DN (RDN)放在一起来生成条目 DN。目录服务器将条目的基本 DN 存储在 cn=userroot,cn=ldbm database,cn=plugins,cn=config 下的数据库后缀配置中，操作属性 nsslapd-suffix。因此，如果您添加了一个 uid=User,ou=PEople,dc=ExaMPlE,DC=COM 条目，但基本 DN 为 ou=people,dc=example,dc=com，则目录服务器在搜索过程中返回 uid=User,ou=people,dc=example,dc=com。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	on
语法	DirectoryString
示例	nsslapd-return-original-entrydn: on

2.1.153. nsslapd-rewrite-rfc1274

此属性已弃用，并将在以后的版本中删除。

此属性仅用于需要属性类型通过 RFC 1274 名称返回的 LDAPv2 客户端。为这些客户端将 的值设为 on。默认值为 off。

2.1.154. nsslapd-rootdn

此属性设置条目的可分辨名称(DN)，不受到访问控制限制、对目录操作的管理限制或常规资源限制。不需要与此 DN 对应的条目，默认情况下，这个 DN 没有条目，因此接受 cn=Directory Manager 等值。

参数	描述
条目 DN	cn=config
有效值	任何有效的可分辨名称
默认值	
语法	DN
示例	nsslapd-rootdn: cn=Directory Manager

2.1.155. nsslapd-rootpw

此属性设置与 Manager DN 关联的密码。当提供 root 密码时，它会根据为 nsslapd-rootpwstoragescheme 属性选择的加密方法进行加密。从服务器控制台查看时，此属性显示值 *。从 dse.ldif 文件查看时，此属性显示加密方法，后跟密码的加密字符串。示例显示 dse.ldif 文件中显示的密码，而不是实际密码。

警告

当在服务器设置时配置根 DN 时，需要一个 root 密码。但是，可以通过直接编辑文件，从 dse.ldif 中删除 root 密码。在这种情况下，根 DN 只能获得对该目录的相同访问，才能进行匿名访问。当为数据库配置了根 DN 时，始终确保在 dse.ldif 中定义 root 密码。pwdhash 命令行工具可以创建新的 root 密码。

重要

从命令行重置目录管理器的密码时，*请勿在* 密码中使用大括号({})。root 密码以 *{password-storage-scheme}hashed_password* 格式保存。大括号中的任何字符都由服务器解释为 root 密码的密码存储方案。如果该文本不是有效的存储方案，或者未正确哈希后的密码，则 Directory Manager 无法绑定到服务器。

参数	描述
条目 DN	cn=config
有效值	任何有效的密码，由 第 6.3.44 节 “密码存储方案” 描述的任何加密方法加密。
默认值	
语法	DirectoryString {*encryption_method* }*encrypted_Password*
示例	nsslapd-rootpw: {SSHA}9Eko69APCJfF

2.1.156. nsslapd-rootpwstoragescheme

此属性设定用于加密 **nsslapd-rootpw** 属性中存储的目录服务器管理器密码的方法。详情请查看 第 6.3.44 节 “密码存储方案”。

此设置不需要重启服务器才能生效。

参数	描述
条目 DN	cn=config
有效值	请参阅 第 6.3.44 节 “密码存储方案”。
默认值	PBKDF2-SHA512
语法	DirectoryString
示例	nsslapd-rootpwstoragescheme: PBKDF2-SHA512

2.1.157. nsslapd-rundir

此参数设置目录服务器在其中存储运行时信息的目录的绝对路径，如 PID 文件。该目录必须由 Directory Server 用户和组所有。只有此用户和组必须在这个目录中具有读写访问权限。

必须重启该服务才能使此属性生效。

参数	描述
条目 DN	cn=config
有效值	Directory 服务器用户可写入的任何目录
默认值	/var/run/dirsrv/
语法	DirectoryString
示例	nsslapd-rundir: /var/run/dirsrv/

2.1.158. nsslapd-sasl-mapping-fallback

默认情况下，只检查第一个匹配的 SASL 映射。如果这个映射失败，则绑定操作也会失败，即使还有其他匹配的映射可能已经正常工作。SASL 映射回退将持续检查所有匹配的映射。

您不必重启服务器才能使此设置生效。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-sasl-mapping-fallback: off

2.1.159. nsslapd-sasl-max-buffer-size

此属性设置最大 SASL 缓冲区大小。

参数	描述
条目 DN	cn=config
有效值	0 到最大 32 位整数值(2147483647)

参数	描述
默认值	67108864 (64 KB)
语法	整数
示例	nsslapd-sasl-max-buffer-size: 67108864

2.1.160. nsslapd-saslpath

设置包含 Cyrus-SASL SASL2 插件的目录的绝对路径。设置此属性可让服务器使用自定义或非标准 SASL 插件库。这通常在安装过程中正确设置，红帽强烈建议不要更改此属性。如果属性不存在或者值为空，这意味着目录服务器使用系统提供的 SASL 插件库，它们是正确的版本。

如果设置了此参数，服务器将使用指定的路径来加载 SASL 插件。如果没有设置此参数，服务器将使用 SASL_PATH 环境变量。如果没有设置 nsslapd-saslpath 或 SASL_PATH，服务器将从默认位置加载 SASL 插件 /usr/lib/sasl2。

对此属性所做的更改不会生效，直到服务器重启为止。

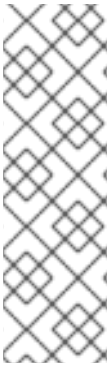
参数	描述
条目 DN	cn=config
有效值	插件目录的路径。
默认值	依赖平台
语法	DirectoryString
示例	nsslapd-saslpath: /usr/lib/sasl2

2.1.161. nsslapd-schemacheck

此属性设置在添加或修改条目时是否强制实施数据库模式。当此属性的值为 时，目录服务器不会检查现有条目的架构，直到它们被修改为止。数据库架构定义数据库中允许的信息类型。默认架构可以使用对象类和属性类型扩展。

警告

红帽强烈建议不要关闭模式检查。这可能导致严重的互操作性问题。这通常用于必须导入到目录服务器中的非常旧的或非标准 LDAP 数据。如果没有大量具有此问题的条目，请考虑在这些条目中使用 scalableObject 对象类来根据每个条目禁用 schema 检查。



注意

在使用 LDAP 客户端进行数据库修改时，架构检查默认可以正常工作，如 ldapmodify，或使用 ldif2db 从 LDIF 导入数据库。如果关闭了 schema 检查，则必须手动验证每个条目，以查看它们是否符合该架构。如果打开了架构检查，服务器会发送一条错误消息，其中列出了与架构不匹配的条目。确保 LDIF 语句中创建的属性和对象类都正确拼写，并在 dse.ldif 中识别。在 schema 目录中创建 LDIF 文件，或将元素添加到 99user.ldif。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	on
语法	DirectoryString
示例	nsslapd-schemacheck: on

2.1.162. nsslapd-schemadir

这是包含特定于 Directory 服务器实例模式文件的目录的绝对路径。当服务器启动时，它会从这个目录中读取模式文件，以及通过 LDAP 工具修改模式时，会更新此目录中的模式文件。该目录必须由服务器用户 ID 所有，并且该用户必须具有目录的读写权限。

对此属性所做的更改不会生效，直到服务器重启为止。

参数	描述
条目 DN	cn=config
有效值	任何有效的路径
默认值	/etc/dirsrv/*instance_name*/schema
语法	DirectoryString
示例	nsslapd-schemadir: /etc/dirsrv/*instance_name*/schem

2.1.163. nsslapd-schema-ignore-trailing-spaces

忽略对象类名称中的结尾空格。默认情况下关闭属性。如果目录包含以一个或多个空格结尾的对象类值的条目，请打开此属性。最好删除尾部空格，因为 LDAP 标准不允许它们。

出于性能原因，需要重新启动服务器才能使更改生效。

当包含尾部空格的对象类添加到条目时，默认会返回一个错误。另外，在添加、修改和导入等操作期间（当对象类扩展并且添加缺失的优越时），忽略尾随空格（如果适用）。这意味着，即使 nsslapd-schema-ignore-trailing-spaces 位于，即使 top 已有值（如 top ）不会被添加。如果找不到对象类并且包含尾随空格，则会记录错误消息并返回到客户端。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-schema-ignore-trailing-spaces: on

2.1.164. nsslapd-schemamod

在线模式修改需要锁定保护，这会影响性能。如果禁用了模式修改，将此参数设置为 off 可以提高性能。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	on
语法	DirectoryString
示例	nsslapd-schemamod: on

2.1.165. nsslapd-schemareplace

决定在 cn=schema 条目中是否允许替换属性值的操作。

参数	描述
条目 DN	cn=config
有效值	on | off | replication-only
默认值	replication-only
语法	DirectoryString
示例	nsslapd-schemareplace: replication-only

2.1.166. nsslapd-search-return-original-type-switch

如果传递给搜索的属性列表包含空格，后接其他字符，则同一字符串将返回到客户端。例如：

```
# ldapsearch -b <basedn> "(filter)" "sn someothertext"
dn: <matched dn>
sn someothertext: <sn>
```

这个行为默认为禁用，但可使用此配置参数启用。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-search-return-type-switch: off

2.1.167. nsslapd-securelistenhost

此属性允许多个目录服务器实例在多主目录计算机上运行（或者，可以限制侦听多主目录计算机的一个接口）。单个主机名可以有多个 IP 地址，这些 IP 地址可以是 IPv4 和 IPv6 的组合。这个参数可用于将 Directory 服务器实例限制为单个 IP 接口；此参数还特别设定用于 TLS 流量的接口，而不是常规 LDAP 连接。

如果为主机名提供 nsslapd-securelistenhost 值，则目录服务器会响应与主机名关联的每个接口的请求。如果给出一个 IP 接口(IPv4 或 IPv6)作为 nsslapd-securelistenhost 值，目录服务器只响应发送到该特定接口的请求。可以使用 IPv4 或 IPv6 地址。

必须重启服务器才能使此属性生效。

参数	描述
条目 DN	cn=config
有效值	任何安全主机名、IPv4 或 IPv6 地址
默认值	
语法	DirectoryString
示例	nsslapd-securelistenhost: ldaps.example.com

2.1.168. nsslapd-securePort

此属性设置用于 TLS 通信的 TCP/IP 端口号。这个所选端口在主机系统中必须是唯一的；确保其他应用程序不会尝试使用相同的端口号。指定小于 1024 的端口号要求以 root 用户身份启动目录服务器。服务

器在启动时将其 uid 设置为 nsslapd-localuser 值。

如果服务器配置了私钥和证书，并且 nsslapd-security 设置为 on，则服务器才会侦听此端口。否则，它不会侦听此端口。

必须重新启动服务器，才能考虑端口号更改。

参数	描述
条目 DN	cn=config
有效范围	1 到 65535
默认值	636
语法	整数
示例	nsslapd-securePort: 636

2.1.169. nsslapd-securitylog-compress

目录服务器默认压缩轮转的安全日志。使用 nsslapd-securitylog-compress 属性来管理安全日志文件压缩。

您不需要重新启动服务器以应用更改。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	on
语法	DirectoryString
示例	nsslapd-securitylog-compress: on

2.1.170. nsslapd-security

此属性设置目录服务器是否接受其加密端口上的 TLS 通信。此属性应设置为 上的，以进行安全连接。要使用安全性运行，除了其他 TLS 配置外，还必须使用私钥和服务器证书配置服务器。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-security: off

2.1.171. nsslapd-securitylog

nsslapd-securitylog 属性设置专用安全日志的路径和文件名，该日志记录身份验证攻击、授权问题、DOS/TCP 攻击和其他安全事件。

要启用安全日志记录，nsslapd-securitylog 属性必须具有有效的路径，并且 nsslapd-securitylog-logging-enabled 配置属性必须在 上 设置为。

参数	描述
条目 DN	cn=config
有效值	任何有效的文件名
默认值	/var/log/dirsrv/slapd-*instance_name*/security
语法	DirectoryString
示例	nsslapd-securitylog: /var/log/dirsrv/slapd-*instance_name*/security

2.1.172. nsslapd-securitylog-list

nsslapd-securitylog-list 属性提供安全日志文件列表。

参数	描述
条目 DN	cn=config
有效值	
默认值	无
语法	DirectoryString
示例	nsslapd-securitylog-list: securitylog2,securitylog3

2.1.173. nsslapd-securitylog-logbuffering

当设置为 off 时，服务器会将所有安全日志条目直接写入磁盘。使用缓冲时，即使负载过重，服务器也使用安全日志，而不影响性能。但是，在调试时，禁用缓冲区以查看操作及其结果，而不必等待日志条目刷新到文件中。禁用日志缓冲可能会严重影响大量载入的服务器的性能。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	on
语法	DirectoryString
示例	nsslapd-security-logbuffering: on

2.1.174. nsslapd-securitylog-logging-enabled

nsslapd-securitylog-logging-enabled 属性打开和关闭安全日志记录。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	on

参数	描述
语法	DirectoryString
示例	nsslapd-security-logging-enabled: on

2.1.175. nsslapd-securitylog-logexpirationtime

nsslapd-securitylog-logexpirationtime 属性设置安全日志文件的最长时间，然后再删除它。

当 nsslapd-securitylog-logexpirationtime 属性提供单元（如 day, week, month 等）时，nsslapd-securitylog-logexpirationtimeunit 属性才会提供单元 的数量。

参数	描述
条目 DN	cn=config
有效范围	-1 到最大 32 位整数值(2147483647) 值为 -1 或 0 表示日志永不过期。
默认值	12
语法	整数
示例	nsslapd-securitylog-logexpirationtime: 12

2.1.176. nsslapd-securitylog-logexpirationtimeunit

nsslapd-securitylog-logexpirationtimeunit 属性设置 nsslapd-securitylog-logexpirationtime 属性的单位。如果您没有为安全日志最长年龄指定单元，或者服务器无法识别该单元，则日志永远不会过期。

参数	描述
条目 DN	cn=config
有效值	month | 周 | 天
默认值	month
语法	DirectoryString

参数	描述
示例	nsslapd-securitylog-logexpirationtimeunit: week

2.1.177. nsslapd-securitylog-logminfreediskspace

nsslapd-securitylog-logminfreediskspace 属性以 MB 为单位设置允许的最小可用磁盘空间。当可用磁盘空间的数量低于此属性中指定的值时，服务器会删除最旧的安全日志，直到出现足够的磁盘空间。

参数	描述
条目 DN	cn=config
有效范围	-1 | 1 到最大 32 位整数值(2147483647)
默认值	5
语法	整数
示例	nsslapd-securitylog-logminfreediskspace: 5

2.1.178. nsslapd-securitylog-logrotationsync-enabled

nsslapd-securitylog-logrotationsync-enabled 属性设置安全日志轮转是否与一天的特定时间同步。以这种方式同步日志轮转，可以在一天（例如每天午夜）的指定时间生成日志文件。这样可以更轻松地分析日志文件，因为它们然后直接映射到日历。

要使安全日志轮转与时间同步，您必须启用 nsslapd-securitylog-logrotationsync-enabled 属性以及配置的 nsslapd-securitylog-logrotationsynchour 和 nsslapd-securitylog-logrotationsyncmin 属性。

例如，要在每天午夜轮转安全日志文件，请通过在 上 将其值设置为，然后将 nsslapd-securitylog-logrotationsynchour 和 nsslapd-securitylog-logrotationsyncmin 属性设为 0 来启用此属性。

参数	描述
条目 DN	cn=config
有效值	on | off

参数	描述
默认值	off
语法	DirectoryString
示例	nsslapd-securitylog-logrotationsync-enabled: off

2.1.179. nsslapd-securitylog-logrotationsynchour

nsslapd-securitylog-logrotationsynchour 属性设置安全日志轮转一天的小时。您必须将属性与 nsslapd-securitylog-logrotationsync-enabled 和 nsslapd-securitylog-logrotationsyncmin 属性一起使用。

参数	描述
条目 DN	cn=config
有效范围	0 到 23
默认值	0
语法	整数
示例	nsslapd-securitylog-logrotationsynchour: 23

2.1.180. nsslapd-securitylog-logrotationsyncmin

nsslapd-securitylog-logrotationsyncmin 属性设置轮转安全日志的当天的分钟。您必须将属性与 nsslapd-securitylog-logrotationsync-enabled 和 nsslapd-securitylog-logrotationsynchour 属性结合使用。

参数	描述
条目 DN	cn=config
有效范围	0 到 59
默认值	0
语法	整数
示例	nsslapd-securitylog-logrotationsyncmin: 30

参数	描述

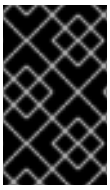
2.1.181. nsslapd-securitylog-logrotationtime

nsslapd-securitylog-logrotationtime 属性设置安全日志文件轮转之间时间的单位 数。使用另一个配置属性 nsslapd-securitylog-logrotationtimeunit 设置单位（天、每周、月份和其他）。

如果 nsslapd-securitylog-maxlogsperdir 属性设置为 1，服务器会忽略 nsslapd-securitylog-logrotationtime 属性。

目录服务器在配置的时间间隔到期后，在第一次写入操作时轮转日志，而不考虑日志的大小。

您可以使用两种方式指定 没有日志轮转 策略。将 nsslapd-securitylog-maxlogsperdir 属性值设置为 1，或者将 nsslapd-securitylog-logrotationtime 属性设置为 -1。服务器首先检查 nsslapd-securitylog-maxlogsperdir 属性，如果属性值大于 1，则服务器会检查 nsslapd-securitylog-logrotationtime 属性。请参阅 第 2.1.171 节 “nsslapd-securitylog” 了解更多信息。



重要

使用 日志轮转 策略会使日志无限期增长，并可能会影响服务器性能。

参数	描述
条目 DN	cn=config
有效范围	-1 | 1 到最大 32 位整数值(2147483647)。-1 值表示安全日志文件轮转之间的时间没有限制。
默认值	1
语法	整数
示例	nsslapd-securitylog-logrotationtime: 5

2.1.182. nsslapd-securitylog-logrotationtimeunit

nsslapd-securitylog-logrotationtimeunit 属性设置 nsslapd-securitylog-logrotationtime （安全日

志轮转时间） 的单位。如果您没有为安全日志轮转策略指定单元，或者服务器无法识别该单元，则日志永远不会过期。

参数	描述
条目 DN	cn=config
有效值	month | week | day | hour | minute
默认值	month
语法	DirectoryString
示例	nsslapd-securitylog-logrotationtimeunit: week

2.1.183. nsslapd-securitylog-maxlogsize

nsslapd-securitylog-maxlogsize 属性以 MB 为单位设置最大安全日志大小。当达到属性值时，Directory 服务器会轮转安全日志，并开始将日志信息写入新日志文件。如果将 nsslapd-securitylog-maxlogsperdir 设置为 1，服务器会忽略 nsslapd-securitylog-maxlogsize 属性。

在设置最大日志大小时，请考虑以下几点：

- 由于日志文件轮转，可以创建的日志文件总数。
- 目录服务器维护五个不同的日志文件：访问日志、审计日志、审计失败日志、错误日志、安全日志。每个日志文件都会消耗磁盘空间。

将这些注意事项与您要为安全日志设置的磁盘空间总量进行比较。

参数	描述
条目 DN	cn=config
有效范围	-1 | 1 到最大 32 位整数值(2147483647)。-1 值表示日志文件的大小没有限制。
默认值	100

参数	描述
语法	整数
示例	nsslapd-securitylog-maxlogsize: 100

2.1.184. nsslapd-securitylog-maxlogsperdir

nsslapd-securitylog-maxlogsperdir 属性设置目录服务器存储在日志文件目录中的安全日志总数。每次轮转安全日志时，都会创建一个新的日志文件。当安全日志目录中包含的文件数量超过 nsslapd-securitylog-maxlogsperdir 属性的值时，目录服务器会删除日志文件的最老版本。

如果 nsslapd-securitylog-maxlogsperdir 属性的值大于 1，请检查 nsslapd-securitylog-logrotationtime 属性，以了解是否设置了日志轮转。如果 nsslapd-securitylog-logrotationtime 属性的值为 -1，则不会发生日志轮转。请参阅 第 2.1.181 节 “nsslapd-securitylog-logrotationtime” 了解更多信息。

参数	描述
条目 DN	cn=config
有效范围	1 到最大 32 位整数值(2147483647)
默认值	10
语法	整数
示例	nsslapd-securitylog-maxlogsperdir: 5

2.1.185. nsslapd-securitylog-mode

nsslapd-securitylog-mode 属性设置目录服务器创建安全日志文件的访问模式或文件权限。有效值是 000 到 777 的组合，因为它们镜像编号或绝对 UNIX 文件权限。该值必须是 3 位数字的组合，数字因 0 到 7 的不同：

- **0 - None**
- **1 - 只执行**

- 2 - 仅写入
- 3 - 写入和执行
- 4 - 只读
- 5 - 读取和执行
- 6 - 读取和写入
- 7 - 读、写和执行

在 3 位数字中，第一个数字代表所有者的权限，第二个数字代表组的权限，第三个数字代表每个人的权限。更改默认值时，请记住 000 不允许访问日志，并且允许每个人的写入权限都可能导致日志被任何人覆盖或删除。

新配置的访问模式仅影响服务器所创建的新日志。当日志轮转到新文件时，会设置模式。

参数	描述
条目 DN	cn=config
有效范围	000 到 777
默认值	600
语法	整数
示例	nsslapd-securitylog-mode: 600

2.1.186. nsslapd-sizelimit

此属性设置从搜索操作返回的最大条目数。如果达到这个限制，ns-slapd 会返回任何与搜索请求匹配的条目，以及超过大小限制错误。

如果没有设置限制，ns-slapd 会将每个匹配条目返回到客户端，而不考虑找到的数量。要设置目录服务器无限期等待搜索完成的限制值，请在 dse.ldif 文件中为此属性指定一个 -1。

这个限制适用于每个人，无论其机构是什么。

注意

dse.ldif 文件中的此属性值 -1 与在服务器控制台中保留属性为空相同，这会导致不使用限制。这无法在 dse.ldif 文件中有一个 null 值，因为它不是有效的整数。可以将其设置为 0， 它会返回 超过每个搜索的大小限制。

对应的 user-level 属性是 nsSizeLimit。

参数	描述
条目 DN	cn=config
有效范围	-1 到最大 32 位整数值(2147483647)
默认值	2000
语法	整数
示例	nsslapd-sizelimit: 2000

2.1.187. nsslapd-snmp-index

此参数控制目录服务器实例的 SNMP 索引号。

如果您在同一主机上有多个目录服务器实例侦听端口 389，但在不同网络接口上，此参数允许您为每个实例设置不同的 SNMP 索引号。

参数	描述
条目 DN	cn=config
有效值	0 到最大 32 位整数值(2147483647)

参数	描述
默认值	0
语法	整数
示例	nsslapd-snmp-index: 0

2.1.188. nsslapd-ssl-check-hostname

此属性设置支持 TLS 的目录服务器是否应该通过与所出示证书中分配给通用名称(cn)属性的值匹配来验证请求的真实性。默认情况下，上的 属性设置为。如果主机名与证书的 cn 属性不匹配，则会记录适当的错误和审计信息。

例如，在复制环境中，如果找到对等服务器的主机名与证书中指定的名称不匹配，则类似以下内容的消息会记录在供应商服务器的日志文件中：

```
[DATE] - SSL alert: ldap_sasl_bind("",LDAP_SASL_EXTERNAL) 81 (Netscape runtime error -
12276 -
Unable to communicate securely with peer: requested domain name does not
match the server's certificate.)

[DATE] NSMMReplicationPlugin - agmt="cn=SSL Replication Agreement to host1"
(host1.example.com:636):
Replication bind with SSL client authentication failed:
LDAP error 81 (Can't contact LDAP server)
```

红帽建议在 上打开此属性来保护目录服务器的出站 TLS 连接，以防出现中间人(MITM)攻击。

注意

必须正确设置 DNS 和反向 DNS 才能正常工作；否则，服务器无法将对等 IP 地址解析为证书中的主题 DN 中的主机名。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	on

参数	描述
语法	DirectoryString
示例	nsslapd-ssl-check-hostname: on

2.1.189. nsslapd-SSLclientAuth

注意

nsslapd-SSLclientAuth 参数将在以后的发行版本中弃用，并当前被维护以向后兼容。使用存储在 cn=encryption,cn=config 下的新参数 nsSSLClientAuth。请参阅 第 2.3.5 节 “nsSSLClientAuth”。

2.1.190. nsslapd-statlog-level

使用 nsslapd-statlog-level 参数在访问日志中启用每个操作的统计信息，而不影响目录服务器性能。

目录服务器支持与搜索操作中使用的索引相关的统计集合。当您将 nsslapd-statlog-level 设置为 1 时，访问日志开始为索引中的每个键收集索引查找数（数据库读取操作）。

例如，一个目录有一个 M uid 条目，其值以 user_ 开头，搜索操作则使用过滤器 (uid=useruildDefaults)。目录服务器创建 ^us，使用、ser 和 er_ 索引键。使用设置 nsslapd-statlog-level=1 时，访问日志会显示以下信息：

```
STAT read index: attribute=uid key(sub)=er_  count 1000000
STAT read index: attribute=uid key(sub)=ser  count 1000000
STAT read index: attribute=uid key(sub)=use  count 1000000
STAT read index: attribute=uid key(sub)=^us  count 1000000
STAT read index: duration 0.001010276
```

了解查找数量和索引查找的整个持续时间有助于诊断为什么过滤器，如 (uid=useruildDefaults)，非常昂贵。

您需要重新启动服务器以应用更改。

参数	描述
条目 DN	cn=config

参数	描述
有效值	• 0 - 无统计数据(collection/log) • 1 - 在搜索操作过程中与索引查找相关的统计信息
默认值	0
语法	整数
示例	nsslapd-statlog-level: 1

2.1.191. nsslapd-syntaxcheck

此属性验证对条目属性的所有修改，以确保新的或更改的值符合该属性类型所需的语法。当启用此属性时，任何不符合正确语法的更改都会被拒绝。所有属性值都会根据 RFC 4514 中的语法定义进行验证。

默认情况下启用此设置。

语法验证仅针对新的或修改后的属性运行；它不会验证现有属性值的语法。为添加和修改等 LDAP 操作触发语法验证；在复制等操作后不会发生语法验证，因为应在原始供应商上检查属性语法的有效性。

这会验证目录服务器的所有支持的属性类型，但二进制语法（无法验证）和非标准语法（没有定义的必要格式）除外。*未验证的* 语法如下：

- 传真（二进制）
- OctetString (binary)
- JPEG (binary)
- 二进制（非标准）

- 空格代表敏感字符串（非标准）
- URI （非标准）

nsslapd-syntaxcheck 属性设定是否验证和拒绝属性修改。这可与 nsslapd-syntaxlogging 属性一起使用，将有关无效属性值的警告信息写入错误日志中。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	on
语法	DirectoryString
示例	nnsslapd-syntaxcheck: on

2.1.192. nsslapd-syntaxlogging

此属性设定是否将语法验证失败记录到错误日志中。默认情况下关闭它。

如果启用了 nsslapd-syntaxcheck 属性（默认），并且还启用了 nsslapd-syntaxlogging 属性，则任何无效的属性更改都会被拒绝，并写入错误日志中。如果只启用 nsslapd-syntaxlogging，并且禁用 nsslapd-syntaxcheck，则允许无效的更改进行，但会在错误日志中写入警告信息。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	nnsslapd-syntaxlogging: off

2.1.193. nsslapd-threadnumber

此与性能调优相关的值设置线程数量，目录服务器在启动时创建。如果值设为 -1 （默认），目录服务器会根据可用的硬件启用优化的自动调整。请注意，如果启用了自动调整，nsslapd-threadnumber 会在目录服务器运行时显示自动生成的线程数量。

注意

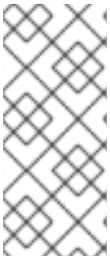
红帽建议使用自动调整设置来优化性能。

参数	描述
条目 DN	cn=config
有效范围	-1 到系统线程和处理器支持的最大线程数。
默认值	-1
语法	整数
示例	nsslapd-threadnumber: -1

2.1.194. nsslapd-timelimit

此属性设置为搜索请求分配的最大秒数。如果达到这个限制，Directory 服务器会返回与搜索请求匹配的任何条目，以及超过的时间限制错误。

如果没有设置限制，ns-slapd 会将每个匹配条目返回到客户端，而不考虑它所需的时间。要设置目录服务器无限期等待搜索完成的限制值，请在 dse.ldif 文件中为此属性指定一个 -1。值为零(0)会导致不允许时间进行搜索。最小时间限制为 1 秒。



注意

dse.ldif 中的此属性值 -1 与在服务器控制台中保留属性 blank 相同，这会导致不使用限制。但是，无法在服务器控制台的此字段中设置负整数，而 null 值无法在 dse.ldif 条目中使用，因为它不是有效的整数。

对应的 user-level 属性是 nsTimeLimit。

参数	描述
条目 DN	cn=config
有效范围	-1 到最大 32 位整数值(2147483647) （以秒为单位）
默认值	3600
语法	整数
示例	nsslapd-timelimit: 3600

2.1.195. nsslapd-tmpdir

这是服务器用于临时文件的目录的绝对路径。目录必须由服务器用户 ID 所有，用户必须具有读写访问权限。没有其他用户 ID 应该对该目录具有读取或写入操作。默认值为 /tmp。

对此属性所做的更改不会生效，直到服务器重启为止。

2.1.196. nsslapd-unhashed-pw-switch

当您更新 userPassword 属性时，Directory 服务器会加密密码并将其存储在 userPassword 中。然而，在某些情况下，例如，当将密码与 Active Directory (AD)同步时，目录服务器必须将未加密的密码传递给插件。在这种情况下，服务器将未加密的密码存储在 so-called 条目扩展 中的临时未哈希的 #user#password 属性中，并根据情况，在 changelog 中。请注意，目录服务器不会在服务器的硬盘 中保存临时未哈希的"${user"密码 属性。

nsslapd-unhashed-pw-switch 参数控制目录服务器是否存储未加密的密码。例如，您必须将 nsslapd-unhashed-pw-switch 设置为 on，以便将 Directory Server 的密码同步到 Active Directory。

您可以将参数设置为以下值之一：

- off ：目录服务器不会在条目扩展或更改日志中存储未加密的密码。如果不使用与 AD 的密码同步，或者任何需要访问未加密的密码的插件，则设置这个值。
- 在 上 ：目录服务器在条目扩展和更改日志中存储未加密的密码。如果您使用 AD 配置密码同步，请设置这个值。

- nolog ：目录服务器仅将未加密的密码存储在条目扩展中，而不存储在 changelog 中。如果本地 Directory 服务器插件需要访问未加密的密码，则设置这个值，但没有配置 AD 的密码同步。

参数	描述
条目 DN	cn=config
有效值	off | on | nolog
默认值	off
语法	DirectoryString
示例	nsslapd-unhashed-pw-switch: off

2.1.197. nsslapd-validate-cert

如果目录服务器配置为在 TLS 中运行，其证书过期，则无法启动目录服务器。nsslapd-validate-cert 参数设置目录服务器在尝试使用过期证书启动时应如何响应：

- warn 允许 Directory 服务器成功使用过期的证书启动，但会发送一条警告信息，但会发送证书已过期的警告信息。这是默认设置。
- on 验证证书，并将阻止服务器在证书过期时重新启动。这会为过期的证书设置硬故障。
- off 禁用所有证书过期验证，因此服务器可以从过期的证书开始，而无需记录警告。

参数	描述
条目 DN	cn=config
有效值	warn | on | off
默认值	warn
语法	DirectoryString
示例	nsslapd-validate-cert: warn

2.1.198. nsslapd-verify-filter-schema

nsslapd-verify-filter-schema 参数定义 Directory 服务器如何使用没有在 schema 中指定的属性验证搜索过滤器。

您可以将 nsslapd-verify-filter-schema 设置为以下选项之一：

- reject-invalid ：如果包含任何未知元素，目录服务器会拒绝带有错误的过滤器。
- process-safe: Directory Server 将未知组件替换为空集，并使用 /var/log/dirsrv/slapd-*instance_name*/access 日志文件中的 notes=F 标志记录警告。

  在将 nsslapd-verify-filter-schema 从 warn-invalid 或 off 切换到 process-safe 之前，请监控访问日志，并修复导致 notes=F 标志的日志条目的查询。否则，操作结果会改变，Directory 服务器可能无法返回所有匹配的条目。
- warn-invalid ：目录服务器使用 /var/log/dirsrv/slapd-*instance_name*/access 日志文件中的 notes=F 标志记录警告，并继续扫描完整的数据库。
- off ：目录服务器不会验证过滤器。

请注意，例如，如果您将 nsslapd-verify-filter-schema 设置为 warn-invalid 或 off，则过滤器 （如 (& (non_exististent_attribute=example) (uid=*user_name*)) 会评估 uid=*user_name* 条目，且仅在它包含 non_existent_attribute=example 时才返回。如果将 nsslapd-verify-filter-schema 设置为 process-safe，目录服务器不会评估该条目，且不会返回它。

注意

将 nsslapd-verify-filter-schema 设置为 reject-invalid 或 process-safe 可防止因为未索引搜索在 schema 中指定的属性造成高负载。

参数	描述
条目 DN	cn=config
有效值	reject-invalid, process-safe, warn-invalid, off

参数	描述
默认值	process-safe
语法	DirectoryString
示例	nsslapd-verify-filter-schema: process-safe

2.1.199. nsslapd-versionstring

此属性设置服务器版本号。当显示 **version** 字符串时，构建数据会自动附加。

参数	描述
条目 DN	cn=config
有效值	任何有效的服务器版本号。
默认值	
语法	DirectoryString
示例	nsslapd-versionstring: Red Hat-Directory/{VER}

2.1.200. nsslapd-workingdir

这是服务器在启动后将 用作其当前工作目录的目录的绝对路径。这是服务器返回 **getcwd** （） 函数的值，系统进程表显示的值显示为其当前工作目录。这是生成核心文件的目录。服务器用户 **ID** 必须具有目录的读写访问权限，而其他用户 **ID** 应该对其具有读取或写入访问权限。此属性的默认值是包含错误日志的目录，通常为 **/var/log/dirsrv/slapd-***实例*。

对此属性所做的更改不会生效，直到服务器重启为止。

2.1.201. nsslapd-numlisteners

nsslapd-numlisteners 属性指定目录服务器可用于监控已建立的连接的监听程序线程数量。您可以通过增加属性值来提高服务器遇到大量客户端连接时的响应时间。

参数	描述
条目 DN	cn=config
有效值	1 - 4
默认值	1
语法	整数
示例	nsslapd-numlisteners: 2

注意

您必须在更改 nsslapd-numlisteners 属性的值后重启服务器。

2.1.202. passwordAdminSkipInfoUpdate

使用 cn=config 条目下的新的 passwordAdminSkipInfoUpdate: on/off 设置，您可以对密码管理员管理的密码更新执行精细的控制。当您在 上将 此设置设置为 时，目录服务器只更新密码，且不更新属性，如 passwordHistory、passwordExpirationTime、passwordRetryCount、pwdReset、passwordExpWarned。

密码管理员可以使用此设置来绕过在使用 passwordExpirationTime 和 pwdMustChange 属性的全局和本地登录策略中配置的密码语法检查和密码过期设置。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	passwordAdminSkipInfoUpdate: on

2.1.203. passwordAllowChangeTime

此属性指定在允许用户更改其密码之前必须经过的时长。

参数	描述
条目 DN	cn=config
有效值	任何整数
默认值	
语法	DirectoryString
示例	passwordAllowChangeTime: 5h

2.1.204. passwordBadWords

passwordBadWords 参数定义一个以逗号分隔的字符串列表，用户不允许在密码中使用。

请注意，目录服务器对字符串进行不区分大小写的比较。

参数	描述
条目 DN	cn=config
有效值	任何字符串
默认值	""
语法	DirectoryString
示例	passwordBadWords: example

2.1.205. passwordChange

指明用户是否可以更改密码。

这可以缩写为 pwdAllowUserChange。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	on
语法	DirectoryString
示例	passwordChange: on

2.1.206. passwordCheckSyntax

此属性设置在保存密码前是否检查密码语法。密码语法检查机制检查密码是否满足或超过密码最小长度要求，并且字符串不包含任何简单词语，如用户名或用户 ID 或存储在 uid、cn、n、gn、geName、ou 或 mail 属性中的任何属性值。

密码语法包括几个不同的类别用于检查：

- 在检查密码中简单词语时要比较的字符串或令牌的长度（例如，如果令牌长度为三个，则用户 UID、名称、电子邮件地址或其他参数中的字符串没有字符串）
- 最小字符数(0-9)
- 最低大写 ASCII 字母字符数
- 最低小写 ASCII 字母字符数
- 最小特殊 ASCII 字符数，如 !@#$
- 最小 8 位字符数
- 每个密码所需的最小字符类别数；类别可以是大写或小写字母、特殊字符、数字或 8 位字符

这可以缩写为 **pwdCheckSyntax**。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	passwordCheckSyntax: off

2.1.207. passwordDictCheck

如果设置为 on，则 passwordDictCheck 参数会根据 CrackLib 字典检查密码。如果新密码包含字典单词，则目录服务器会拒绝密码。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	passwordDictCheck: off

2.1.208. passwordExp

指明用户密码在指定秒数后是否过期。默认情况下，用户密码不会过期。启用密码过期后，使用 passwordMaxAge 属性设置密码过期的秒数。

参数	描述
条目 DN	cn=config
有效值	on | off

参数	描述
默认值	off
语法	DirectoryString
示例	passwordExp: on

2.1.209. passwordExpirationTime

此属性指定在用户密码过期前传递的时间长度。

参数	描述
条目 DN	cn=config
有效值	整数中的任何日期
默认值	none
语法	GeneralizedTime
示例	passwordExpirationTime: 202009011953

2.1.210. passwordExpWarned

此属性表示密码到期警告已发送给用户。

参数	描述
条目 DN	cn=config
有效值	true | false
默认值	none
语法	DirectoryString
示例	passwordExpWarned: true

2.1.211. passwordGraceLimit

此属性仅在启用了密码过期时才适用。用户密码已过期后，服务器允许用户连接更改密码的目的。这称为 *宽限期*。服务器仅允许在完全锁定用户之前进行一定的尝试。此属性是允许的宽限期数量。值 0 表示服务器不允许安全登录。

参数	描述
条目 DN	cn=config
有效值	0 (off)到任何合理的整数
默认值	0
语法	整数
示例	passwordGraceLimit: 3

2.1.212. passwordHistory

启用密码历史记录。密码历史记录指的是是否允许用户重复使用密码。默认情况下禁用密码历史记录，用户可以重复使用密码。如果在 上 将此属性设置为，则目录会存储给定数量的旧密码，并防止用户重复使用任何存储的密码。使用 passwordInHistory 属性设置目录服务器存储的旧密码数量。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	passwordHistory: on

2.1.213. passwordInHistory

表示目录服务器存储在历史记录中的密码数量。用户无法重复使用存储在历史记录中的密码。默认情况下，密码历史记录功能被禁用，这意味着目录服务器不存储任何旧密码，因此用户可以重复使用密码。使用 passwordHistory 属性启用密码历史记录。

要防止用户通过跟踪的密码数量快速循环，请使用 passwordMinAge 属性。

这可以缩写为 **pwdInHistory**。

参数	描述
条目 DN	cn=config
有效范围	1 到 24 个密码
默认值	6
语法	整数
示例	passwordInHistory: 7

2.1.214. passwordIsGlobalPolicy

此属性控制是否复制密码策略属性。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	passwordIsGlobalPolicy: off

2.1.215. passwordLegacyPolicy

启用旧的密码行为。旧的 LDAP 客户端预期在超过最大失败限制后收到一个错误，以锁定用户帐户。*例如，如果限制有三个失败，则帐户在第四个失败尝试时被锁定。但是，较新的客户端可能会在达到失败限制时收到错误消息。例如，如果限制是三个失败，则应在第三个失败尝试时锁定帐户。*

因为在超过失败限制时锁定帐户是旧的行为，所以它被视为旧的行为。它默认是启用的，但可以禁用以允许新的 LDAP 客户端在预期时间收到错误。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	on
语法	DirectoryString
示例	passwordLegacyPolicy: on

2.1.216. passwordLockout

指明用户在给定数量的绑定尝试失败后是否锁定了目录。默认情况下，在一系列绑定尝试失败后，用户不会被锁定在目录中。如果启用了帐户锁定，请设置使用 passwordMaxFailure 属性锁定用户被锁定的绑定尝试次数。

这可以缩写为 pwdLockOut。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	passwordLockout: off

2.1.217. passwordLockoutDuration

表示用户在帐户锁定后锁定目录的时间（以秒为单位）。帐户锁定功能可防止尝试通过重复尝试猜测用户密码来进入该目录的黑客。使用 passwordLockout 属性启用和禁用帐户锁定功能。

这可以缩写为 pwdLockoutDuration。

参数	描述
条目 DN	cn=config
有效范围	1 到最大 32 位整数值(2147483647) （以秒为单位）
默认值	3600
语法	整数
示例	passwordLockoutDuration: 3600

2.1.218. passwordMaxAge

表示用户密码过期的秒数。要使用此属性，必须使用 passwordExp 属性启用密码过期。

这可以缩写为 pwdMaxAge。

参数	描述
条目 DN	cn=config
有效范围	1 到最大 32 位整数值(2147483647) （以秒为单位）
默认值	8640000 (100 天)
语法	整数
示例	passwordMaxAge: 100

2.1.219. passwordMaxClassChars

如果将 passwordMaxClassChars 参数设置为大于 0 的值，Directory 服务器会阻止设置具有比参数中设置的值相同的连续字符的密码。如果启用，Directory 服务器会检查以下类别的连续字符：

- ***数字***
- ***alpha 字符***

- *小写*
- *大写*

例如，如果您将 passwordMaxClassChars 设置为 3，则不允许包含 jdif 或 1947 的密码。

参数	描述
条目 DN	cn=config
有效范围	0 （禁用）最大 32 位整数(2147483647)
默认值	0
语法	整数
示例	passwordMaxClassChars: 0

2.1.220. passwordMaxFailure

表示在用户锁定目录后绑定尝试失败的次数。默认情况下禁用帐户锁定。通过修改 passwordLockout 属性来启用帐户锁定。

这可以缩写为 pwdMaxFailure。

参数	描述
条目 DN	cn=config
有效范围	1 用于最大整数绑定失败
默认值	3
语法	整数
示例	passwordMaxFailure: 3

2.1.221. passwordMaxRepeats

同一字符可以按顺序显示在密码中的最大次数。零(0)已关闭。整数值拒绝任何使用字符超过该次数的密码；例如，1 拒绝一次使用的字符（一个 ）和 2 拒绝字符超过两次(aa)。

参数	描述
条目 DN	cn=config
有效范围	0 到 64
默认值	0
语法	整数
示例	passwordMaxRepeats: 1

2.1.222. passwordMaxSeqSets

如果将 passwordMaxSeqSets 参数设置为大于 0 的值，Directory 服务器会拒绝带有重复 monotonic 序列超过参数中设置的长度的密码。例如，如果您将 passwordMaxSeqSets 设置为 2，则将密码设置为 azXYZ_XYZ-g，因为 XYZ 出现在密码中。

参数	描述
条目 DN	cn=config
有效范围	0 （禁用）到最大 32 位整数值(2147483647)
默认值	0
语法	整数
示例	passwordMaxSeqSets: 0

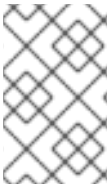
2.1.223. passwordMaxSequence

如果将 passwordMaxSequence 参数设置为大于 0 的值，Directory 服务器会拒绝使用 monotonic 序列的新密码，超过 passwordMaxSequence 中设置的值。例如，如果您将 参数设置为 3，则目录服务器会拒绝包含字符串的密码，如 1234 或 dcba。

参数	描述
条目 DN	cn=config
有效范围	0 （禁用）到最大 32 位整数值(2147483647)
默认值	0
语法	整数
示例	passwordMaxSequence: 0

2.1.224. passwordMin8Bit

这会设置密码必须包含的最小 8 位字符数。



注意

必须禁用对 userPassword 的 7 位检查才能使用它。

参数	描述
条目 DN	cn=config
有效范围	0 到 64
默认值	0
语法	整数
示例	passwordMin8Bit: 0

2.1.225. passwordMinAge

表示在用户更改密码前必须经过的秒数。将此属性与 passwordInHistory （要记住的密码数）一起使用，以防止用户通过密码快速循环，以便他们可以再次使用旧密码。值为零(0)表示用户可以立即更改密码。

这可以缩写为 pwdMaxFailure。

参数	描述
条目 DN	cn=config
有效范围	0 到有效的最大整数
默认值	0
语法	整数
示例	passwordMinAge: 150

2.1.226. passwordMinAlphas

此属性设置最少的字母字符密码数。

参数	描述
条目 DN	cn=config
有效范围	0 到 64
默认值	0
语法	整数
示例	passwordMinAlphas: 4

2.1.227. passwordMinCategories

这将设置密码中代表的最小字符类别数。类别是：

- 小写字母字符
- 大写字母字符
- Number

- 特殊 ASCII 计费，如 $ 和 punctuation 标记
- 8 位字符

例如，如果此属性的值设为 2，并且用户尝试将密码更改为 aaaaa，则服务器将拒绝密码，因为它仅包含小写字符，因此仅包含一个类别中的字符。A AaA 的密码会传递，因为它包含两个类别（大写和小写）中的字符。

默认值为 3，这意味着如果启用了密码语法检查，则有效的密码必须具有三种字符类别。

参数	描述
条目 DN	cn=config
有效范围	0 到 5
默认值	0
语法	整数
示例	passwordMinCategories: 2

2.1.228. PasswordMinDigits

这会设置密码必须包含的最小数字数。

参数	描述
条目 DN	cn=config
有效范围	0 到 64
默认值	0
语法	整数
示例	passwordMinDigits: 3

2.1.229. passwordMinLength

此属性指定目录服务器用户密码属性中必须使用的最小字符数。通常，较短的密码更容易破解。目录服务器强制使用八个字符的最小密码。这很难破解但很短，用户可以在不写出密码的情况下记住密码。

*这可以缩写为 **pwdMinLength**。*

参数	描述
条目 DN	cn=config
有效范围	2 到 512 个字符
默认值	8
语法	整数
示例	passwordMinLength: 8

2.1.230. PasswordMinLowers

此属性设置字符密码必须包含的最小小写字母数。

参数	描述
条目 DN	cn=config
有效范围	0 到 64
默认值	0
语法	整数
示例	passwordMinLowers: 1

2.1.231. PasswordMinSpecials

此属性设置密码必须包含的最小 特殊，或不是字母数字字符。

参数	描述
条目 DN	cn=config
有效范围	0 到 64
默认值	0
语法	整数
示例	passwordMinSpecials: 1

2.1.232. PasswordMinTokenLength

此属性设置用于 简单 词语检查的最小属性值长度。例如，如果 PasswordMinTokenLength 设为 3，则给定名称 DJ 不会造成拒绝 DJ 的策略，但策略会拒绝 DJ 的密码组成了 bob 的 givenName 。

目录服务器根据以下属性中的值检查最小令牌长度：

- *uid*
- *cn*
- *sn*
- *givenName*
- *mail*
- *ou*

如果目录服务器应检查其他属性，您可以在 passwordUserAttributes 参数中设置它们。详情请查看 第 2.1.244 节 “passwordUserAttributes”。

参数	描述
条目 DN	cn=config
有效范围	1 到 64
默认值	3
语法	整数
示例	passwordMinTokenLength: 3

2.1.233. PasswordMinUppers

这设置大写字母密码必须包含的最小大写字母数。

参数	描述
条目 DN	cn=config
有效范围	0 到 64
默认值	0
语法	整数
示例	passwordMinUppers: 2

2.1.234. passwordMustChange

指明用户在首次绑定到目录服务器时或何时由 Manager DN 重置密码时，是否需要更改其密码。

这可以缩写为 pwdMustChange。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off

参数	描述
语法	DirectoryString
示例	passwordMustChange: off

2.1.235. passwordPalindrome

如果启用了 passwordPalindrome 参数，如果新密码包含 palindrome，目录服务器会拒绝密码。

palindrome 是一个字符串，它读取与后相同的转发，如 abc11cba。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	passwordPalindrome: off

2.1.236. passwordResetFailureCount

表示密码失败计数器重置的时间（以秒为单位）。每次从用户帐户发送无效的密码时，密码失败计数器都会递增。如果在 上将 passwordLockout 属性设置为 on，则当计数器达到 passwordMaxFailure 属性指定的故障数量（默认为 600 秒）时，用户会被锁定。在 passwordLockoutDuration 属性指定的时间长度后，失败计数器将重置为零(0)。

这可以缩写为 pwdFailureCountInterval。

参数	描述
条目 DN	cn=config
有效范围	1 到最大 32 位整数值(2147483647) （以秒为单位）
默认值	600

参数	描述
语法	整数
示例	passwordResetFailureCount: 600

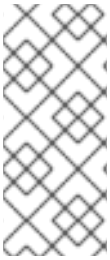
2.1.237. passwordSendExpiringTime

当客户端请求密码过期时，Directory 服务器仅在密码位于警告期间时返回"time to expire"值。为提供始终期望返回这个值的现有客户端的兼容性 - 无论密码过期时间是否在警告期间内 - passwordSendExpiringTime 参数可以设为 on。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	passwordSendExpiringTime: off

2.1.238. passwordStorageScheme

此属性设定用于加密存储在 userPassword 属性中的用户密码的方法。详情请查看 第 6.3.44 节 “密码存储方案”。



注意

红帽建议不要设置此属性。如果没有设置值，Directory 服务器会自动使用最强支持的密码存储方案。如果将来的目录服务器更新更改了默认值以提高安全性，如果用户设置密码，则会自动使用新的存储方案加密密码。

此设置不需要重启服务器才能生效。

参数	描述

参数	描述
条目 DN	cn=config
有效值	请查看 第 6.3.44 节 “密码存储方案”
默认值	PBKDF2-SHA512
语法	DirectoryString
示例	passwordStorageScheme: PBKDF2-SHA512

2.1.239. passwordTPRDelayExpireAt

passwordTPRDelayExpireAt 属性是密码策略的一部分。当管理员将临时密码设置为用户帐户后，passwordTPR DelayExpireAt 会在临时密码过期前定义时间（以秒为单位）。

此设置不需要重启服务器才能生效。

参数	描述
条目 DN	cn=config
有效值	-1（禁用）到最大 32 位整数值(2147483647)
默认值	-1
语法	整数
示例	passwordTPRDelayExpireAt: 3600

2.1.240. passwordTPRDelayValidFrom

passwordTPRDelayValidFrom 属性是密码策略的一部分。当管理员将临时密码设置为用户帐户后，password TPRDelayValidFrom 定义可以使用临时密码前的时间（以秒为单位）。

此设置不需要重启服务器才能生效。

参数	描述
条目 DN	cn=config
有效值	-1（禁用）到最大 32 位整数值(2147483647)
默认值	-1
语法	整数
示例	passwordTPRDelayValidFrom: 60

2.1.241. passwordTPRMaxUse

passwordTPRMaxUse 属性是密码策略的一部分。属性设置用户成功验证的次数，或者在临时密码过期前无法验证。如果身份验证成功，目录服务器仅允许用户在进行其他操作前更改密码。如果用户没有更改密码，则操作将终止。无论身份验证是成功，验证尝试次数的计数器都会增加。

此设置不需要重启服务器才能生效。

参数	描述
条目 DN	cn=config
有效值	-1（禁用）到最大 32 位整数值(2147483647)
默认值	-1
语法	整数
示例	passwordTPRMaxUse: 5

2.1.242. passwordTrackUpdateTime

设置是否记录一个单独的时间戳，特别是最后一次更改条目密码的时间。如果启用了，它会将 pwdUpdateTime 操作属性添加到用户帐户条目（与其它更新时间（如 modifyTime）添加。

使用这个时间戳可以更轻松地在不同 LDAP 存储（如 Active Directory）间同步密码更改。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	passwordTrackUpdateTime: off

2.1.243. passwordUnlock

指明用户是否被锁定在指定时间内被锁定的目录，或直到管理员在帐户锁定后重置密码为止。帐户锁定功能可防止尝试通过重复尝试猜测用户密码来破坏目录的恶意参与者。如果此 passwordUnlock 属性设置为 off，并且操作属性 accountUnlockTime 的值为 0， 则帐户将无限期锁定。

参数	描述
条目 DN	cn=config
有效值	on | off
默认值	on
语法	DirectoryString
示例	passwordUnlock: off

2.1.244. passwordUserAttributes

默认情况下，如果您在 passwordMinTokenLength 参数中设置了最小令牌长度，Directory 服务器只检查特定属性的令牌。详情请查看 第 2.1.232 节 “PasswordMinTokenLength”。

passwordUserAttributes 参数允许您设置目录服务器应检查的额外属性的逗号分隔列表。

参数	描述
条目 DN	cn=config

参数	描述
有效值	任何字符串
默认值	""
语法	DirectoryString
示例	passwordUserAttributes: telephoneNumber, l

2.1.245. passwordWarning

表示用户密码之前的秒数，因为用户在下次 LDAP 操作中收到密码过期警告控制。根据 LDAP 客户端，在发送警告时，用户也可以提示更改密码。

这可以缩写为 ***pwdExpireWarning。***

参数	描述
条目 DN	cn=config
有效范围	1 到最大 32 位整数值(2147483647) （以秒为单位）
默认值	86400 (1 天)
语法	整数
示例	passwordWarning: 86400

2.1.246. retryCountResetTime

retryCountResetTime 属性包含 UTC-format 中的日期和时间，在 passwordRetryCount 属性将重置为 0 后。

参数	描述
条目 DN	cn=config
有效范围	任何 UTC 格式的有效时间戳
默认值	none

参数	描述
语法	常规时间
示例	retryCountResetTime: 20190618094419Z

2.2. 更改属性

changelog 属性包含在 changelog 中记录的更改。

2.2.1. changeLog

此属性包含条目的可分辨名称，其中包含由服务器的 changelog 组成的一组条目。

OID	2.16.840.1.113730.3.1.35
语法	DN
multi- 或 Single-Valued	多值
定义在	changelog Internet Draft

2.2.2. changeNumber

此属性始终存在。它包含一个整数，用于唯一标识对目录条目所做的每个更改。这个数字与更改发生的顺序相关。数值越大，稍后的更改。

OID	2.16.840.1.113730.3.1.5
语法	整数
multi- 或 Single-Valued	多值
定义在	changelog Internet Draft

2.2.3. 更改

此属性包含对以 LDIF 格式添加和修改操作的条目所做的更改。

OID	2.16.840.1.113730.3.1.8
语法	二进制
multi- 或 Single-Valued	多值
定义在	changelog Internet Draft

2.2.4. changeTime

当添加条目时，此属性以 YYMMDDHHMMSS 格式定义一个时间。

OID	2.16.840.1.113730.3.1.77
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	目录服务器

2.2.5. changeType

此属性指定 LDAP 操作的类型，添加、删除、修改 或 modrdn。例如：

> *changeType: modify*

OID	2.16.840.1.113730.3.1.7
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	changelog Internet Draft

2.2.6. deleteOldRdn

对于 modrdn 操作，此属性指定是否删除旧 RDN。

值为零(0)将删除旧的 RDN。任何其它非零值都会保留旧的 RDN。（非零值可以是负整数或正整数。）

OID	2.16.840.1.113730.3.1.10
语法	布尔值
multi- 或 Single-Valued	多值
定义在	changelog Internet Draft

2.2.7. filterInfo

这供 changelog 用于处理复制。

OID	2.16.840.1.113730.3.1.206
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	目录服务器

2.2.8. newRdn

对于 modrdn 操作，此属性指定条目的新 RDN。

OID	2.16.840.1.113730.3.1.9
语法	DN
multi- 或 Single-Valued	多值
定义在	changelog Internet Draft

2.2.9. newSuperior

对于 modrdn 操作，此属性为移动条目指定新的父(superior)条目。

OID	2.16.840.1.113730.3.1.11

语法	DN
multi- 或 Single-Valued	多值
定义在	changelog Internet Draft

2.2.10. targetDn

此属性包含受 LDAP 操作影响的条目的 DN。对于 modrdn 操作，targetDn 属性在修改或移动前包含条目的 DN。

OID	2.16.840.1.113730.3.1.6
语法	DN
multi- 或 Single-Valued	多值
定义在	changelog Internet Draft

2.3. CN=ENCRYPTION,CN=CONFIG

加密相关属性存储在 cn=encryption,cn=config 条目下。cn=encryption,cn=config 条目是 nsslapdEncryptionConfig 对象类的实例。

2.3.1. allowWeakCipher

此属性控制允许或拒绝弱密码。默认值取决于 nsSSL3Ciphers 参数中设置的值。

密码被认为较弱，如果：

- 它们是可导出的。

  可导出的密码在密码名称中被标记为 EXPORT。例如，在 TLS_RSA_EXPORT_WITH_RC4_40_MD5 中。

- 它们比 3DES 算法的对称和更弱。

对于加密和解密，对称加密都使用相同的加密密码。

- *密钥长度比 128 位短。*

必须重启服务器才能使此属性生效。

条目 DN	cn=encryption,cn=config
有效值	on | off
默认值	**off**，如果 **nsSSL3Ciphers** 参数中的值被设置为 **+all** 或 **default**。 **在 上**，如果 **nsSSL3Ciphers** 参数的值包含特定于用户的加密列表。
语法	DirectoryString
示例	allowWeakCipher: on

2.3.2. allowWeakDHParam

与目录服务器关联的网络安全服务(NSS)库至少需要 2048 位 Diffie-Hellman (DH)参数。但是，一些客户端连接到目录服务器（如 Java 1.6 和 1.7 客户端）只支持 1024 位 DH 参数。allowWeakDHParam 参数允许您启用对目录服务器中弱 1024 位 DH 参数的支持。

必须重启服务器才能使此属性生效。

参数	描述
条目 DN	cn=encryption,cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	allowWeakDHParam: off

2.3.3. nsSSL3Ciphers

此属性指定加密目录服务器在加密通信过程中使用的集合。

*此参数中设置的值会影响 **allowWeakCipher** 参数的默认值。详情请查看 第 2.3.1 节 “allowWeakCipher”。*

参数	描述
条目 DN	cn=encryption,cn=config
有效值	以逗号分隔的 NSS 支持的密码列表。另外，还可使用以下参数： * 默认：启用 NSS 公告的默认密码，除了弱密码除外。如需更多信息，请参阅 列出 SSL 连接支持的密码套件。 * +all ：所有密码都已启用。如果启用了 **allowWeakCipher** 参数，这包括弱密码。 * -all ：所有密码都被禁用。
默认值	default
语法	DirectoryString 使用加号(**+**)符号启用或减号(**-**)符号来禁用，后跟密码。密码列表中不允许使用空格。 要启用除 **rsa_null_md5** 以外的所有密码 - 必须特别调用 - 指定 **+all**。
示例	nsSSL3Ciphers: +TLS_RSA_AES_128_SHA,+TLS_RSA_AES_256_SHA, +TLS_RSA_WITH_AES_128_GCM_SHA256,-RSA_NULL_SHA

2.3.4. nsSSLActivation

*此属性显示是否为给定安全模块启用 **TLS** 密码系列。*

条目 DN	cn=*encryptionType*,cn=encryption,cn=config
有效值	on | off

默认值	
语法	DirectoryString
示例	nsSSLActivation: on

2.3.5. nsSSLClientAuth

此属性显示目录服务器如何强制实施客户端身份验证。它接受以下值：

- off - 目录服务器不接受客户端身份验证
- allowed （默认）- 目录服务器将接受客户端身份验证，但不需要它
- 必需 - 所有客户端都必须使用客户端身份验证。

必须重启服务器才能使此属性生效。

参数	描述
条目 DN	cn=config
有效值	off | 允许 | 必需
默认值	allowed
语法	DirectoryString
示例	nsSSLClientAuth: allowed

2.3.6. nsSSLEnabledCiphers

目录服务器自动生成多值 nsSSLEnabledCiphers 属性。属性是只读的，显示 Directory 服务器当前使用的密码。列表可能与您在 nsSSL3Ciphers 属性中设置的相同。例如，如果您在 nsSSL3Ciphers 属性中设置了弱密码，但 allowWeakCipher 被禁用，则 nsSSLEnabledCiphers 属性不会列出弱密码，也不会使用它们。

参数	描述
条目 DN	cn=config
有效值	此属性的值是自动生成的和只读。
默认值	
语法	DirectoryString
示例	nsSSLClientAuth: TLS_RSA_WITH_AES_256_CBC_SHA::AES::SHA1::256

2.3.7. nsSSLPersonalitySSL

此属性包含用于 SSL 的证书名称。

条目 DN	cn=encryption,cn=config
有效值	证书 nickname
默认值	
语法	DirectoryString
例如：	nsSSLPersonalitySSL: Server-Cert

2.3.8. nsSSLSessionTimeout

此属性设置 TLS 连接的生命周期持续时间。最小超时值为 5 秒。如果设置了较小的值，则会自动被 5 秒替代。大于有效范围内的最大值的值由范围内的最大值替换。

必须重启服务器才能使此属性生效。

参数	描述
条目 DN	cn=encryption,cn=config
有效范围	5 秒到 24 小时

参数	描述
默认值	0，这意味着使用上面有效范围内的最大值。
语法	整数
示例	nsSSLSessionTimeout: 5

2.3.9. nsSSLSupportedCiphers

此属性包含服务器支持的密码。

条目 DN	cn=encryption,cn=config
有效值	特定的系列、密码和强度字符串
默认值	
语法	DirectoryString
例如：	nsSSLSupportedCiphers: TLS_RSA_WITH_AES_256_CBC_SHA::AES::SHA1::256

2.3.10. nsSSLToken

此属性包含服务器使用的令牌（安全模块）的名称。

条目 DN	cn=encryption,cn=config
有效值	模块名称
默认值	
语法	DirectoryString
例如：	nsSSLToken: internal （软件）

2.3.11. nsTLS1

启用 TLS 版本 1。与 TLS 使用的密码在 nsSSL3Ciphers 属性中定义。

如果将 sslVersionMin 和 sslVersionMax 参数与 nsTLS1 结合使用，Directory 服务器会从这些参数中选择最安全的设置。

必须重启服务器才能使此属性生效。

参数	描述
条目 DN	cn=encryption,cn=config
有效值	on | off
默认值	on
语法	DirectoryString
示例	nsTLS1: on

2.3.12. nsTLSAllowClientRenegotiation

目录服务器使用 SSL_OptionSet （） 网络安全服务(NSS)功能以及 SSL_ENABLE_RENEGOTIATION 选项来控制 NSS 的 TLS 重新协商行为。

nsTLSAllowClientRenegotiation 属性控制目录服务器传递给 SSL_ENABLE_RENEGOTIATION 选项的值：

- 如果您在 上设置了 nsTLSAllowClientRenegotiation:，则目录服务器会将 SSL_RENEGOTIATE_REQUIRES_XTN 传递给 SSL_ENABLE_RENEGOTIATION 选项。在这种情况下，NSS 允许使用 RFC 5746 进行安全重新协商尝试。
- 如果您设置了 nsTLSAllowClientRenegotiation: off，目录服务器会将 SSL_RENEGOTIATE_NEVER 传递给 SSL_ENABLE_RENEGOTIATION 选项。在这种情况下，NSS 会拒绝所有重新协商尝试，甚至是安全的尝试。

有关 NSS TLS 重新协商行为的详情，请查看 NSS 中的 RFC 5746 实现（网络安全服务） 部分，红帽是否受 TLS 重新协商 MITM 攻击(CVE-2009-3555)? 文章。

必须重启该服务才能使此属性生效。

参数	描述
条目 DN	cn=encryption,cn=config
有效值	on | off
默认值	on
语法	DirectoryString
示例	nsTLSAllowClientRenegotiation: on

2.3.13. sslVersionMax

设置要使用的 TLS 协议的最大版本。默认情况下，这个值被设置为系统中安装的 NSS 库中最新可用协议版本。

必须重启服务器才能使此属性生效。

如果将 sslVersionMin 和 sslVersionMax 参数与 nsTLS1 结合使用，Directory 服务器会从这些参数中选择最安全的设置。

条目 DN	cn=encryption,cn=config
有效值	TLS 协议版本，如 **TLS1.0**
默认值	在系统中安装的 NSS 库中的最新可用协议版本
语法	DirectoryString
例如：	sslVersionMax: TLS1.2

2.3.14. sslVersionMin

sslVersionMin 参数设置 TLS 协议 Directory 服务器使用的最小版本。但是，默认情况下，Directory 服务器根据系统范围的加密策略自动设置此参数。如果您在 /etc/crypto-policies/config 文件中将加密策略配置集设置为：

- *DEFAULT、FUTURE 或 FIPS，目录服务器将 sslVersionMin 设置为 TLS1.2*

- *LEGACY, Directory Server 将 sslVersionMin 设置为 TLS1.0*

或者，您可以手动将 sslVersionMin 设置为高于加密策略中定义的值。

必须重启该服务才能使此属性生效。

条目 DN	cn=encryption,cn=config
有效值	TLS 协议版本，如 **TLS1.2**
默认值	取决于您设置的系统范围的加密策略配置集。
语法	DirectoryString
例如：	sslVersionMin: TLS1.2

2.4. CN=FEATURES,CN=CONFIG

cn=features 条目本身没有属性。此条目仅用作父容器条目，以及 nsContainer 对象类。

子条目包含一个 oid 属性，用于识别功能和 directoryServerFeature 对象类，以及有关该功能的可选识别信息，如特定的 ACL。例如：

```
dn: oid=2.16.840.1.113730.3.4.9,cn=features,cn=config
objectClass: top
objectClass: directoryServerFeature
oid: 2.16.840.1.113730.3.4.9
cn: VLV Request Control
aci: (targetattr != "aci")(version 3.0; acl "VLV Request Control"; allow( read, search, compare,
proxy ) userdn = "ldap:///all";)
creatorsName: cn=server,cn=plugins,cn=config
modifiersName: cn=server,cn=plugins,cn=config
createTimestamp: 20210129132357Z
modifyTimestamp: 20210129132357Z
```

2.4.1. OID

oid 属性包含分配给目录服务功能的对象标识符。OID 被用作这些目录功能的 naming 属性。

OID	2.16.840.1.113730.3.1.215
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	目录服务器

2.5. CN=MAPPING TREE,CN=CONFIG

- 后缀、复制和 Windows 同步的配置属性存储在 cn=mapping tree,cn=config 下。与后缀相关的配置属性可在后缀 subentry cn=suffix,cn=mapping tree,cn=config 下找到。

  例如，后缀 是目录树中的 root 条目，如 dc=example,dc=com。

- 复制配置属性存储在 cn=replica,cn=后缀,cn=mapping tree,cn=config 下。

- 复制协议属性存储在 cn='replicationAgreementName,cn=replica,cn=suffix,cn=mapping tree,cn=config 下。

- Windows 同步协议属性存储在 cn=syncAgreementName,cn=replica,cn=suffix,cn=mapping tree,cn=config 下。

2.6. CN=SUFFIX_DN,CN=MAPPING TREE,CN=CONFIG

后缀配置存储在 cn-suffix_DN,cn-mapping tree,cn-config 条目中。这些条目是 nsMappingTree 对象类的实例。scalableObject 对象类启用属于它的条目存放任何用户属性。对于服务器要考虑的后缀配置属性，除了 顶级 对象类外，这些对象类也必须存在于条目中。

您必须用引号编写后缀 DN，因为它包含等号(=)、逗号(,)和空格字符等字符。通过使用引号，DN 可以正确地作为另一个 DN 中的值。例如： cn-"dc=example,dc=com",cn-mapping tree,cn-config

2.6.1. cn

此强制属性设置新后缀的相对可分辨名称(RDN)。

参数	描述
条目 DN	cn=*suffix_DN*,cn=mapping tree,cn=config
有效值	任何有效的 LDAP DN
默认值	
语法	DirectoryString
示例	cn: dn=example,dc=com

2.6.2. nsslapd-backend

此参数设置用于处理请求的数据库或数据库链接的名称。它是多值，每个值有一个数据库或数据库链接。当 nsslapd-state 属性的值设置为 backend 或 update 时引用时，需要 此属性。

将值设为 cn=ldbm database,cn=plugins,cn=config 下的后端数据库条目实例的名称。例如：o=userroot,cn=ldbm database,cn=plugins,cn=config

参数	描述
条目 DN	cn=*suffix_DN*,cn=mapping tree,cn=config
有效值	任何有效的分区名称
默认值	
语法	DirectoryString
示例	nsslapd-backend: userRoot

2.6.3. nsslapd-distribution-function

nssldap-distribution-function 参数设置自定义分发函数的名称。当您在 nsslapd-backend 属性中设置多个数据库时，您必须设置此属性。

参数	描述
条目 DN	cn=*suffix_DN*,cn=mapping tree,cn=config

参数	描述
有效值	任何有效的发布功能
默认值	
语法	DirectoryString
示例	nsslapd-distribution-plugin: distribution_function_name

2.6.4. nsslapd-distribution-plugin

nssldap-distribution-plugin 设置用于自定义分发功能的共享库。当您在 nsslapd-backend 属性中设置多个数据库时，您必须设置此属性。

参数	描述
条目 DN	cn=*suffix_DN*,cn=mapping tree,cn=config
有效值	任何有效的发布插件
默认值	
语法	DirectoryString
示例	nsslapd-distribution-plugin: /path/to/shared/library

2.6.5. nsslapd-parent

如果要创建子后缀，请使用 nsslapd-parent 属性来定义父后缀。

如果没有设置属性，则以 root 后缀的形式创建新的后缀。

参数	描述
条目 DN	cn=*suffix_DN*,cn=mapping tree,cn=config
有效值	任何有效的分区名称
默认值	

参数	描述
语法	DirectoryString
示例	nsslapd-parent-suffix: dc=example,dc=com

2.6.6. nsslapd-referral

此属性设置后缀返回的引用的 LDAP URL。您可以多次添加 nssldap-referral 属性来设置多个引用 URL。

如果将 nsslapd-state 参数设置为 referral 或 update，则必须设置此属性。

参数	描述
条目 DN	cn=*suffix_DN*,cn=mapping tree,cn=config
有效值	任何有效的 LDAP URL
默认值	
语法	DirectoryString
示例	nssldap-referral: ldap://example.com/

2.6.7. nsslapd-state

这个参数决定了后缀如何处理操作。属性采用以下值：

- 后端 ：后端数据库处理所有操作。
- disabled ：数据库不可用于处理操作。服务器会返回 No such search 对象 错误，以响应客户端应用程序发出的请求。
- 引用 ：目录服务器返回对此后缀的请求引用 URL。

- *引用更新 ： 数据库用于所有操作。只有更新请求才会被发送一个引用。*

参数	描述
条目 DN	cn=*suffix_DN*,cn=mapping tree,cn=config
有效值	后端 | 禁用 | 引用 | 更新引用
默认值	后端
语法	DirectoryString
示例	nsslapd-state: backend

2.7. CN=REPLICA,CN=SUFFIX_DN,CN=MAPPING TREE,CN=CONFIG

复制配置属性存储在 cn-replica,cn-suffix,cn-mapping tree,cn-config 下。cn-replica 条目是 nsDS5Replica 对象类的实例。对于服务器要考虑的复制配置属性，该条目中必须存在此对象类（除 顶级对象类之外）。

cn-replica,cn-suffix,cn-mapping tree,cn-config 条目必须包含以下对象类：

- *top*
- *extensibleObject*
- *nsds5replica*

2.7.1. cn

设置副本的 naming 属性。cn 属性必须设置为 replica。

参数	描述
条目 DN	cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config

参数	描述
有效值	该值必须设置为 **副本**。
默认值	replica
语法	DirectoryString
示例	cn=replica

2.7.2. nsds5DebugReplicaTimeout

此属性提供在使用带有调试日志记录运行时使用的替代超时时间。这只能设置时间和 debug 级别：

> ***nsds5debugreplicatimeout: seconds[:debuglevel]***

参数	描述
条目 DN	cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	任何数字字符串
默认值	
语法	DirectoryString
示例	nsds5debugreplicatimeout: 60:8192

2.7.3. nsDS5Flags

此属性设置之前在标记中定义的副本属性。目前只有一个标志，它设定日志更改。

参数	描述
条目 DN	cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	0 | 1 * *0* ：副本不会写入更改日志 ; 这是消费者的默认设置。 * *1：* 副本写入更改日志 ; 这是 hub 和供应商的默认设置。

参数	描述
默认值	0
语法	整数
示例	nsDS5Flags: 0

2.7.4. nsDS5ReplConflict

虽然此属性不在 cn=replica 条目中，但它与复制结合使用。此多值属性包含在具有更改冲突的条目中，这些冲突无法被同步过程自动解决。要检查需要管理员干预的复制冲突，请执行 LDAP 搜索 (nsDS5ReplConflict.4-1.)。例如：

```
# ldapsearch -D "cn=Directory Manager" -W -p 389 -h server.example.com -x -s sub -b
dc=example,dc=com "(|(objectclass=nsTombstone)(nsDS5ReplConflict=*))" dn
nsDS5ReplConflict nsUniqueID
```

使用搜索过滤器 " (objectclass=nsTombstone) " 也显示 tombstone (deleted)条目。nsDS5ReplConflict 的值包含有关冲突哪些条目的更多信息，通常是通过其 nsUniqueID 引用它们。可以通过其 nsUniqueID 搜索 tombstone 条目。例如：

```
# ldapsearch -D "cn=Directory Manager" -W -p 389 -h server.example.com -x -s sub -b
dc=example,dc=com "(|(objectclass=nsTombstone)(nsUniqueID=66a2b699-1dd211b2-
807fa9c3-a58714648))"
```

2.7.5. nsDS5ReplicaAbortCleanRUV

此 read-only 属性指定删除过时或缺失供应商的旧 RUV 条目的后台任务是否中止。有关此任务的更多信息，请参阅 第 2.7.22 节 “nsDS5ReplicaTombstonePurgeInterval”。值 0 表示任务不活跃，值 1 表示任务处于活跃状态。

此属性存在，允许在服务器重启后恢复 abort 任务。任务完成后，属性会被删除。

如果手动设置这个值，服务器会忽略修改请求。

参数	描述
条目 DN	cn=replica,cn=suffixDN,cn=mapping tree,cn=config

参数	描述
有效值	0 | 1
默认值	无
语法	整数
示例	nsDS5ReplicaAbortCleanRUV: 1

2.7.6. nsDS5ReplicaAutoReferral

此属性设置 Directory 服务器是否遵循为数据库配置引用。

参数	描述
条目 DN	cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	on | off
默认值	
语法	DirectoryString
示例	nsDS5ReplicaAutoReferral: on

2.7.7. nsds5ReplicaBackoffMin 和 nsds5ReplicaBackoffMax

这些属性用于具有大量复制流量的环境中使用，其中更新需要尽快发送。

默认情况下，如果远程副本忙碌，复制协议将进入"back off"状态，它将重试以在 back-off 计时器的下一个间隔发送更新。默认情况下，计时器从 3 秒启动，最长等待期限为 5 分钟。因为这些默认设置在某些情况下可能不足，所以您可以使用 nsds5ReplicaBackoffMin 和 nsds5ReplicaBackoffMax 来配置最小和最大等待时间。

配置设置可以在服务器在线时应用，不需要重新启动服务器。如果使用无效的设置，则使用默认值。配置必须通过 CLI 工具处理。

2.7.8. nsDS5ReplicaBindDN

这个多值属性指定在绑定时要使用的 DN。虽然这个 cn=replica 条目中可以有多个值，但每个复制协议只能有一个供应商绑定 DN。每个值都应该是消费者服务器上本地条目的 DN。如果复制供应商使用基于客户端证书的身份验证来连接到消费者，请在消费者上配置证书的证书映射，将证书中的 subjectDN 映射到本地条目。

重要

为安全起见，请不要将此属性设置为 cn=Directory Manager。

参数	描述
条目 DN	cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	任何有效的 DN
默认值	
语法	DirectoryString
示例	nsDS5ReplicaBindDN: cn=replication manager,cn=config

2.7.9. nsDS5ReplicaBindDNGroup

nsDS5ReplicaBindDNGroup 属性指定组 DN。然后，这个组会被扩展，其成员（包括其子组的成员）在启动时或修改副本对象时添加到 replicaBindDNs 属性中。这会扩展 nsDS5ReplicaBindDN 属性提供的当前功能，因为它允许设置组 DN。

参数	描述
条目 DN	cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	任何有效的组 DN
默认值	
语法	DirectoryString
示例	nsDS5ReplicaBindDNGroup: cn=sample_group,ou=groups,dc=example,dc=com

2.7.10. nsDS5ReplicaBindDNGroupCheckInterval

目录服务器检查 nsDS5ReplicaBindDNGroup 属性中指定的组中的任何更改，并相应地自动重建 replicaBindDN 参数的列表。这些操作对性能有负面影响，因此仅在 nsDS5ReplicaBindDNGroupCheckInterval 属性中设置的指定间隔执行。

此属性接受以下值：

- *-1 ：在运行时禁用动态检查。当 nsDS5ReplicaBindDNGroup 属性更改时，管理员必须重启实例。*
- *0: 目录服务器在更改组后立即重建列表。*
- *任何正 32 位整数值：自上次重建以来传递所需的最小秒数。*

参数	描述
条目 DN	cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	-1 到最大 32 位整数(2147483647)
默认值	-1
语法	整数
示例	nsDS5ReplicaBindDNGroupCheckInterval: 0

2.7.11. nsDS5ReplicaChangeCount

此 read-only 属性显示更改日志中的条目总数，以及它们是否仍然被复制。当更改日志被清除时，只有仍然要复制的条目会保留。

请参阅] 和 xref:ref_nsDS5ReplicaTombstonePurgeInterval_assembly_cn-replica-cn-suffix_dn-cn-mapping-tree-cn-config[以了解有关清除操作属性的更多信息。

参数	描述
条目 DN	cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config

参数	描述
有效范围	-1 到最大 32 位整数(2147483647)
默认值	
语法	整数
示例	nsDS5ReplicaChangeCount: 675

2.7.12. nsDS5ReplicaCleanRUV

此 read-only 属性指定删除过时或缺失供应商的旧 RUV 条目的后台任务是否活跃。有关此任务的更多信息，请参阅 第 2.26 节 “cn=task_name,cn=abort cleanallruv,cn=tasks,cn=config”。值 0 表示任务不活跃，值 1 表示任务处于活跃状态。

此属性存在，允许在服务器重启后恢复清理任务。任务完成后，属性会被删除。

如果手动设置这个值，服务器会忽略修改请求。

参数	描述
条目 DN	cn=replica,cn=suffixDN,cn=mapping tree,cn=config
有效值	0 | 1
默认值	无
语法	整数
示例	nsDS5ReplicaCleanRUV: 0

2.7.13. nsDS5ReplicaId

此属性为给定复制环境中的供应商设置唯一 ID。

参数	描述
条目 DN	cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config

参数	描述
有效范围	对于供应商： **1** 到 **65534** 对于消费者和中心：655 **35**
默认值	
语法	整数
示例	nsDS5ReplicaId: 1

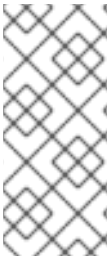
2.7.14. nsDS5ReplicaLegacyConsumer

如果此属性不存在或值为 false，这表示副本不是传统的消费者。

参数	描述
条目 DN	cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	true | false
默认值	false
语法	DirectoryString
示例	nsDS5ReplicaLegacyConsumer: false

2.7.15. nsDS5ReplicaName

此属性指定内部操作具有唯一标识符的副本名称。如果没有指定，则在创建副本时，此唯一标识符由服务器分配。



注意

建议允许服务器生成此名称。然而，在某些情况下，例如，在 replica 角色更改了（为 hub 等提供），需要指定这个值。否则，服务器将不会使用正确的更改日志数据库，复制会失败。

此属性仅用于内部使用。

参数	描述
条目 DN	cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	
默认值	
语法	DirectoryString (UID 标识副本)
示例	nsDS5ReplicaName: 66a2b699-1dd211b2-807fa9c3-a58714648

2.7.16. nsds5ReplicaProtocolTimeout

*在停止服务器、禁用复制或删除复制协议时，在服务器负载下停止复制前需要等待的超时时间。**nsds5ReplicaProtocolTimeout** 属性可用于配置此超时，其默认值为 **120 秒**。*

*有些情况下，超时为 **2 分钟**的时间过长，或者不够长。例如，在关闭过程中结束复制会话前，特定的复制协议可能需要更多时间。*

此属性可以添加到后端的主复制配置条目中：

参数	描述
条目 DN	cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping tree,cn=config
有效范围	0 到最大 32 位整数(2147483647) （以秒为单位）
默认值	120
语法	整数
示例	nsds5ReplicaProtocolTimeout: 120

nsds5ReplicaProtocolTimeout 属性也可以添加到复制协议中。复制协议协议超时会覆盖主副本配置条目中设置的超时。这允许不同的复制协议进行不同的超时。如果复制会话正在进行，则一个新的超时将中止该会话并允许服务器关闭。

2.7.17. nsDS5ReplicaPurgeDelay

此属性控制已删除条目(tombstone 条目)和状态信息的最长期限。

目录服务器存储 tombstone 条目和状态信息，以便在多层次复制过程中发生冲突时，服务器会根据存储在更改序列号中的时间戳和副本 ID 解决冲突。

内部目录服务器日常操作会定期删除比此属性值旧的 tombstone 条目（以秒为单位）。当修改包含状态信息的条目时，会删除除 nsDS5ReplicaPurgeDelay 值旧的状态信息的信息。

并非所有 tombstone 和状态信息都可能会被删除，因为带有多层次复制功能，服务器可能需要保留少量对 prime 复制的最新更新，即使它们比属性值旧。

此属性指定在条目上执行内部清除操作的时间间隔（以秒为单位）。在设置此属性时，请确保清除延迟比复制策略中的最长复制周期长，以保留足够信息来解决复制冲突，并防止在不同服务器中存储的数据副本被分离。

参数	描述
条目 DN	cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效范围	0 （永久保留）最大 32 位整数(2147483647)
默认值	604800 [1 week (60x60x24x7)]
语法	整数
示例	nsDS5ReplicaPurgeDelay: 604800

2.7.18. nsDS5ReplicaReapActive

这个 read-only 属性指定从数据库中删除旧 tombstones （删除条目）的后台任务是否活跃。有关此任务的更多信息，请参阅 第 2.7.22 节 “nsDS5ReplicaTombstonePurgeInterval”。值 0 表示任务不活跃，值 1 表示任务处于活跃状态。如果手动设置这个值，服务器会忽略修改请求。

参数	描述
条目 DN	cn=replica,cn=suffixDN,cn=mapping tree,cn=config
有效值	0 | 1

参数	描述
默认值	
语法	整数
示例	nsDS5ReplicaReapActive: 0

2.7.19. nsDS5ReplicaReferral

这个多值属性指定用户定义的引用。这应该只在消费者上定义。只有客户端试图修改只读消费者中的数据时，才会返回用户引用。此可选引用覆盖由复制协议使用者自动配置的引用。

URL 可以使用格式 ldap://host_name:port_number 或 ldap://IP_address:port_number，带有 IPv4 或 IPv6 地址。

参数	描述
条目 DN	cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	任何有效的 LDAP URL
默认值	
语法	DirectoryString
示例	nsDS5ReplicaReferral: ldap://server.example.com:389

2.7.20. nsDS5ReplicaReleaseTimeout

此属性在多层次场景中供应商和 hub 上使用时，会决定供应商发布副本的超时时间（以秒为单位）。当问题（如网络连接较慢）时，这非常有用，导致一个供应商获得对一个副本的访问并长时间保存，从而导致所有其他供应商访问并发送更新。如果设置了此属性，则副本由供应商在指定周期后发布，从而提高了复制性能。

将此属性设置为 0 可禁用超时。其他任何值都决定超时时间（以秒为单位）。

重要

避免将此属性设置为 1 到 30 之间的值。在大多数情况下，简短的超时会降低复制性能。

参数	描述
条目 DN	cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	0 到最大 32 位整数(2147483647) （以秒为单位）
默认值	60
语法	整数
示例	nsDS5ReplicaReleaseTimeout: 60

2.7.21. nsDS5ReplicaRoot

此属性在复制区域的根目录中设置 DN。此属性的值必须与被复制的数据库的后缀相同，且无法修改。

参数	描述
条目 DN	cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	要复制的数据库的后缀，即后缀 DN
默认值	
语法	DirectoryString
示例	nsDS5ReplicaRoot: "dc=example,dc=com"

2.7.22. nsDS5ReplicaTombstonePurgeInterval

此属性指定清除操作周期之间的时间间隔（以秒为单位）。

服务器定期运行内部内务操作，以从 changelog 和主数据库清除旧的更新和状态信息。请参阅 第 2.7.17 节 “nsDS5ReplicaPurgeDelay”。

在设置此属性时，请记住清除操作非常耗时，特别是在服务器处理来自客户端和供应商的多个删除操作时。

参数	描述
条目 DN	cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效范围	0 到最大 32 位整数(2147483647) （以秒为单位）
默认值	86400 (1 天)
语法	整数
示例	nsDS5ReplicaTombstonePurgeInterval: 86400

2.7.23. nsDS5ReplicaType

定义此副本和其它副本之间存在的复制关系类型。

参数	描述
条目 DN	cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	0 | 1 | 2 | 3 * *0* 表示未知 * *1* 表示主（尚未使用） * *2* 表示消费者（只读） * *3* 个消费者/供应商（更新）
默认值	
语法	整数
示例	nsDS5ReplicaType: 2

2.7.24. nsds5Task

此属性启动复制任务，如将数据库内容转储到 LDIF 文件或从复制拓扑中删除过时的供应商。

您可以将 nsds5Task 属性设置为以下值之一：

- *cl2ldif ：将 changelog 导出到 /var/lib/dirsrv/slapd-instance_name/changelogdb/ 目录中的 LDIF 文件。*
- *ldif2cl ：从存储在 /var/lib/dirsrv/slapd-instance_name/changelogdb/ 目录中的 LDIF 文件导入 changelog。*
- *cleanruv ：从运行操作的供应商中删除 Replica Update Vector (RUV)。*
- *cleanallruv ：从复制拓扑中的所有服务器中删除 RUV。*

您不必重启服务器才能使此设置生效。

参数	描述
条目 DN	cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	* **cl2ldif** * **ldif2cl** * **cleanruv** * **cleanallruv**
默认值	
语法	DirectoryString
示例	nsds5Task: cleanallruv

2.7.25. nsState

此属性存储时钟状态的信息。它仅用于内部用途，以确保服务器无法生成更改序列号(csn) inferior 到检测向后兼容性错误所需的现有序列号。

2.8. CN=REPLICATIONAGREEMENTNAME,CN=REPLICA,CN=SUFFIX_DN,CN=MAPPING TREE,CN=CONFIG

涉及复制协议的复制属性存储在 cn=ReplicationAgreementName,cn=replica,cn=suffix_DN,cn=mapping tree,cn=config 下。cn=ReplicationAgreementName 条目是 nsDS5ReplicationAgreement 对象类的实例。复制协议仅在供应商副本上配置。

2.8.1. cn

此属性用于命名。设定了此属性后，它就无法修改。设置复制协议需要此属性。

参数	描述
条目 DN	cn=*ReplicationAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	任何有效的 **cn**
默认值	
语法	DirectoryString
示例	cn: SupplierAtoSupplierB

2.8.2. description

对复制协议的自由格式文本描述。可以修改此属性。

参数	描述
条目 DN	cn=*ReplicationAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	任何字符串
默认值	
语法	DirectoryString
示例	描述 ：服务器 A 和服务器 B 之间的复制协议。

2.8.3. nsDS50ruv

此属性存储从此复制协议的消费者读取的最后一个副本更新向量(RUV)。它始终存在，不得更改。

2.8.4. nsDS5BeginReplicaRefresh

初始化副本。默认情况下，此属性不存在。但是，如果添加此属性的值为 **start**，则服务器会初始化副本并删除属性值。要监控初始化过程的状态，请轮询此属性。初始化完成后，属性会从条目中删除，其他监控属性可用于详细状态查询。

参数	描述
条目 DN	cn=*ReplicationAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	stop | start
默认值	
语法	DirectoryString
示例	nsDS5BeginReplicaRefresh: start

2.8.5. nsDS5ReplicaBindDN

此属性设置在复制期间绑定到消费者时要使用的 **DN**。此属性的值必须与消费者副本的 **cn=replica** 中的相同。如果使用基于证书的验证，这可能为空，在这种情况下，使用的 **DN** 是证书的主题 **DN**，并且消费者必须启用适当的客户端证书映射。也可以修改它。

参数	描述
条目 DN	cn=*ReplicationAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	任何有效的 DN （如果使用客户端证书，则可以是空的）
默认值	
语法	DirectoryString
示例	nsDS5ReplicaBindDN: cn=replication manager,cn=config

2.8.6. nsDS5ReplicaBindMethod

此属性设置服务器用来绑定到消费者服务器的方法。

nsDS5ReplicaBindMethod 支持以下值：

- 空或 SIMPLE ：服务器使用基于密码的身份验证。使用此绑定方法时，还要设置 nsds5ReplicaBindDN 和 nsds5ReplicaCredentials 参数，以提供用户名和密码。
- SSLCLIENTAUTH ：启用供应商和消费者之间的基于证书的身份验证。为此，使用者服务器必须配置有证书映射，以将供应商的证书映射到复制管理器条目。
- sasl/GSSAPI ：使用 SASL 启用 Kerberos 身份验证。这要求供应商服务器具有 Kerberos keytab，并且消费者服务器配置为将供应商的 Kerberos 主体映射到复制管理器条目。
- SASL/DIGEST-MD5 ：使用带 DIGEST-MD5 机制的 SASL 启用基于密码的身份验证。使用此绑定方法时，还要设置 nsds5ReplicaBindDN 和 nsds5ReplicaCredentials 参数，以提供用户名和密码。

参数	描述
条目 DN	cn=*ReplicationAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	SIMPLE | SSLCLIENTAUTH | SASL/GSSAPI | SASL/DIGEST
默认值	SIMPLE
语法	DirectoryString
示例	nsDS5ReplicaBindMethod: SIMPLE

2.8.7. nsds5ReplicaBootstrapBindDN

当供应商因为 LDAP_INVALID_CREDENTIALS (err=32)错误而绑定到消费者时，nsds 5ReplicaBootstrapBindDN 参数设置回退绑定区分名称(DN)，或者 LDAP_ NO_SUCH_OBJECT (err=32) 错误。

*在这些情况下，目录服务器使用 **nsds5ReplicaBootstrapBindDN,nsds5ReplicaBootstrapCredentials,nsds5ReplicaBootstrapBindMethod, 和 nsds5ReplicaBootstrapTransportInfo 参数中的信息来建立连接。如果服务器也无法使用这些 bootstrap 设置建立连接，服务器会停止尝试连接。***

参数	描述
条目 DN	cn=*ReplicationAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	任何有效的 DN
默认值	
语法	DirectoryString
示例	nsds5ReplicaBootstrapBindDN: cn=replication manager,cn=config

2.8.8. nsds5ReplicaBootstrapBindMethod

*当供应商因为 **LDAP_INVALID_CREDENTIALS (err=32)错误而绑定到消费者时， ns ds 5ReplicaBootstrapBindMethod 参数为回退登录机制 设定密码。***

*在这些情况下，目录服务器使用 **nsds5ReplicaBootstrapBindDN,nsds5ReplicaBootstrapCredentials,nsds5ReplicaBootstrapBindMethod, 和 nsds5ReplicaBootstrapTransportInfo 参数中的信息来建立连接。如果服务器也无法使用这些 bootstrap 设置建立连接，服务器会停止尝试连接。***

参数	描述
条目 DN	cn=*ReplicationAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	SIMPLE | SSLCLIENTAUTH | SASL/GSSAPI | SASL/DIGEST
默认值	
语法	DirectoryString
示例	nsds5ReplicaBootstrapBindMethod: SIMPLE

2.8.9. nsds5ReplicaBootstrapCredentials

当供应商无法绑定到消费者，因为 LDAP_INVALID_CREDENTIALS (err =32)错误，当供应商无法绑定到消费者时，nsds 5ReplicaBootstrapCredentials 参数为回退绑定名称(DN) 设置密码。

在这些情况下，目录服务器使用 nsds5ReplicaBootstrapBindDN,nsds5ReplicaBootstrapCredentials,nsds5ReplicaBootstrapBindMethod, 和 nsds5ReplicaBootstrapTransportInfo 参数中的信息来建立连接。如果服务器也无法使用这些 bootstrap 设置建立连接，服务器会停止尝试连接。

当您以明文设置参数时，目录服务器使用 AES 反向密码加密算法自动哈希密码。

参数	描述
条目 DN	cn=*ReplicationAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	任何有效的字符串。
默认值	
语法	DirectoryString
示例	nsds5ReplicaBootstrapCredentials: password

2.8.10. nsds5ReplicaBootstrapTransportInfo

当供应商因为 LDAP_INVALID_CREDENTIALS (err=49)、LDAP_INAPPROPRIATE_AUTH (err=48)、或 LDAP_NO_SUCH_OBJECT (err=JECT) (32T)错误，或 LDAP_INAPPROPRIATE_AUTH (err=48)、或 LDAP_NO_SUCH_OBJECT (err=JECT) 错误时，Directory 服务器使用的 nsds5ReplicaBootstrapTransportInfo 参数设置连接的加密方法。

在这些情况下，目录服务器使用 nsds5ReplicaBootstrapBindDN,nsds5ReplicaBootstrapCredentials,nsds5ReplicaBootstrapBindMethod, 和 nsds5ReplicaBootstrapTransportInfo 参数中的信息来建立连接。如果服务器也无法使用这些 bootstrap 设置建立连接，服务器会停止尝试连接。

属性采用以下值：

- ***TLS: 连接使用 StartTLS 命令启动加密。***
- ***SSL ：连接使用带有 TLS 加密的 LDAPS。***
- ***LDAP ：连接没有加密。***

参数	描述
条目 DN	cn=*ReplicationAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	TLS | SSL | LDAP
默认值	
语法	DirectoryString
示例	nsds5ReplicaBootstrapTransportInfo: SSL

2.8.11. nsDS5ReplicaBusyWaitTime

此属性设置供应商在消费者发送回忙响应后等待的时间（以秒为单位），然后再进行另一个尝试获取访问。默认值为 3 秒。如果属性设为负值，Directory 服务器会向客户端发送一条消息，以及 LDAP_UNWILLING_TO_PERFORM 错误代码。

nsDS5ReplicaBusyWaitTime 属性与 nsDS5ReplicaSessionPauseTime 属性一起工作。有两个属性被设计，因此 nsDS5ReplicaSessionPauseTime 间隔至少比 nsDS5ReplicaBusyWaitTime 指定的时间间隔至少一秒。较长的时间间隔可让等待供应商更好地获得消费者访问，然后以前的供应商可以重新访问消费者。

使用 changetype:modify 和 replace 操作，随时设置 nsDS5ReplicaBusyWaitTime 属性。如果已在进行中，则更改会对下一个更新会话生效。

参数	描述
条目 DN	cn=*ReplicationAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	任何有效的整数

参数	描述
默认值	3
语法	整数
示例	nsDS5ReplicaBusyWaitTime: 3

2.8.12. nsDS5ReplicaChangesSentSinceStartup

此 read-only 属性显示自服务器启动以来发送到此副本的更改数量。属性中的实际值存储为二进制 blob。

在命令行中，属性值以二进制形式显示。例如：

```
nsds5replicaChangesSentSinceStartup:: MToxLzAg
```

参数	描述
条目 DN	cn=*ReplicationAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效范围	0 到最大 32 位整数(2147483647)
默认值	
语法	整数
示例	nsds5replicaChangesSentSinceStartup:: MToxLzAg

2.8.13. nsDS5ReplicaCredentials

此属性为 nsDS5ReplicaBindDN 属性中指定的绑定 DN 设置凭证。目录服务器使用此密码连接到消费者。

以下示例显示了加密值，如存储在 /etc/dirsrv/slapd-instance_name/dse.ldif 文件中，而不是实际密码。要设置值，请使用明文设置，如 nsDS5ReplicaCredentials: password。目录服务器随后在存储值时使用 AES 反向密码加密模式加密密码。

当使用基于证书的身份验证时，此属性没有设置值。

参数	描述
条目 DN	cn=*ReplicationAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	任何有效的密码
默认值	
语法	DirectoryString {AES-*Base64-algorithm-id*}*encoded_password*
示例	nsDS5ReplicaCredentials: {AES-TUhNR0NT... }VoglUB8GG5A...

2.8.14. nsds5ReplicaEnabled

此属性设定复制协议是否活跃，这意味着每个协议是否发生复制。默认为 on，以便启用复制。

参数	描述
条目 DN	cn=*ReplicationAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	on | off
默认值	on
语法	DirectoryString
示例	nsds5ReplicaEnabled: off

2.8.15. nsds5ReplicaFlowControlPause

在达到 nsds5ReplicaFlowControlWindow 参数中设置的条目数量和更新后，这个参数会将时间（以毫秒为单位）设置为 pause。更新 nsds5ReplicaFlowControlWindow 和 nsds5ReplicaFlowControlPause 参数可让您微调复制吞吐量。详情请查看 第 2.8.16 节 “nsds5ReplicaFlowControlWindow”。

此设置不需要重启服务器才能生效。

参数	描述
条目 DN	cn=*replication_agreement_name*,cn=replica,cn=*suffix_DN*,cn=mapping tree,cn=config
有效值	0 到最大 64 位长
默认值	2000
语法	整数
示例	nsds5ReplicaFlowControlPause: 2000

2.8.16. nsds5ReplicaFlowControlWindow

此属性设置供应商发送的最大条目数和更新，它们没有被消费者确认。达到限制后，供应商会暂停 nsds5ReplicaFlowControlPause 参数中设置的时间的复制协议。更新 nsds5ReplicaFlowControlWindow 和 nsds5ReplicaFlowControlPause 参数可让您微调复制吞吐量。

如果供应商发送条目和更新速度快于消费者导入或更新，并且确认数据，则更新此设置。在这种情况下，供应商的错误日志文件中会记录以下信息：

> ***Total update flow control gives time (2000 msec) to the consumer before sending more entries [msgid sent: xxx, rcv: yyy])***
> ***If total update fails you can try to increase nsds5ReplicaFlowControlPause and/or decrease nsds5ReplicaFlowControlWindow in the replica agreement configuration***

此设置不需要重启服务器才能生效。

参数	描述
条目 DN	cn=*replication_agreement_name*,cn=replica,cn=*suffix_DN*,cn=mapping tree,cn=config
有效值	0 到最大 64 位长
默认值	1000
语法	整数

参数	描述
示例	nsds5ReplicaFlowControlWindow: 1000

2.8.17. nsDS5ReplicaHost

此属性为包含消费者副本的远程服务器设置主机名。设定了此属性后，它就无法修改。

参数	描述
条目 DN	cn=*ReplicationAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	任何有效的主机名
默认值	
语法	DirectoryString
示例	nsDS5ReplicaHost: ldap2.example.com

2.8.18. nsDS5ReplicaLastInitEnd

此可选的 read-only 属性在消费者副本初始化结束时的状态。

参数	描述
条目 DN	cn=*ReplicationAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	*yyyymmddHHMMSSZ* 是打开连接的 Generalized Time 表单的日期/时间。这个值提供了与 Greenwich Mean Time 相关的时间。小时设置 24 小时时钟。末尾的 **Z** 表示时间相对于 Greenwich Mean Time。
默认值	
语法	GeneralizedTime
示例	nsDS5ReplicaLastInitEnd: 20200504121603Z

2.8.19. nsDS5ReplicaLastInitStart

此可选的 read-only 属性在启动消费者副本时的状态。

参数	描述
条目 DN	cn=*ReplicationAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	*yyyymmddHHMMSSZ* 是打开连接的 Generalized Time 表单的日期/时间。这个值提供了与 Greenwich Mean Time 相关的时间。小时设置 24 小时时钟。末尾的 **Z** 表示时间相对于 Greenwich Mean Time。
默认值	
语法	GeneralizedTime
示例	nsDS5ReplicaLastInitStart: 20200503030405

2.8.20. nsDS5ReplicaLastInitStatus

此可选的 read-only 属性提供消费者初始化的状态。通常有一个数字代码，后跟一个简短字符串，说明其状态。零(0)表示成功。

参数	描述
条目 DN	cn=*ReplicationAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	0 (consumer Initialization Succeeded)，后跟任何其他状态消息。
默认值	
语法	字符串
示例	nsDS5ReplicaLastInitStatus: 0 Consumer Initialization Succeeded

2.8.21. nsDS5ReplicaLastUpdateEnd

此只读属性会在最新复制调度更新结束时显示。

参数	描述
条目 DN	cn=*ReplicationAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	*yyyymmddHHMMSSZ* 是打开连接的 Generalized Time 表单的日期/时间。这个值提供了与 Greenwich Mean Time 相关的时间。小时设置 24 小时时钟。末尾的 **Z** 表示时间相对于 Greenwich Mean Time。
默认值	
语法	GeneralizedTime
示例	nsDS5ReplicaLastUpdateEnd: 20200502175801Z

2.8.22. nsDS5ReplicaLastUpdateStart

此只读属性会在最新复制调度更新启动时显示。

参数	描述
条目 DN	cn=*ReplicationAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	*yyyymmddHHMMSSZ* 是打开连接的 Generalized Time 表单的日期/时间。这个值提供了与 Greenwich Mean Time 相关的时间。小时设置 24 小时时钟。末尾的 **Z** 表示时间相对于 Greenwich Mean Time。
默认值	
语法	GeneralizedTime
示例	nsDS5ReplicaLastUpdateStart: 20200504122055Z

2.8.23. nsds5replicaLastUpdateStatus

在每个复制协议的 read-only nsds5replicaLastUpdateStatus 属性中，Directory 服务器会显示协议的最新状态。

参数	描述
条目 DN	cn=*ReplicationAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	任何有效的复制协议状态
默认值	
语法	DirectoryString
示例	nsds5replicaLastUpdateStatus: Error (0) Replica successfully: Incremental update succeeded

2.8.24. nsDS5ReplicaPort

此属性设置包含副本的远程服务器的端口号。设定了此属性后，它就无法修改。

参数	描述
条目 DN	cn=*ReplicationAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	包含副本的远程服务器的端口号
默认值	
语法	整数
示例	nsDS5ReplicaPort:389

2.8.25. nsds5ReplicaProtocolTimeout

在停止服务器、禁用复制或删除复制协议时，在服务器负载下停止复制前需要等待的超时时间。nsds5ReplicaProtocolTimeout 属性可用于配置此超时，其默认值为 120 秒。

有些情况下，超时为 2 分钟的时间过长，或者不够长。例如，在关闭过程中结束复制会话前，特定的复制协议可能需要更多时间。

此属性可以添加到后端的主复制配置条目中：

参数	描述
条目 DN	cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping tree,cn=config
有效范围	0 到最大 32 位整数(2147483647) （以秒为单位）
默认值	120
语法	整数
示例	nsds5ReplicaProtocolTimeout: 120

nsds5ReplicaProtocolTimeout 属性也可以添加到复制协议中。复制协议协议超时会覆盖主副本配置条目中设置的超时。这允许不同的复制协议进行不同的超时。如果复制会话正在进行，则一个新的超时将中止该会话并允许服务器关闭。

2.8.26. nsDS5ReplicaReapActive

这个 read-only 属性指定从数据库中删除旧 tombstones （删除条目）的后台任务是否活跃。有关此任务的更多信息，请参阅 第 2.7.22 节 “nsDS5ReplicaTombstonePurgeInterval”。值为零(0)表示任务不活跃，值 1 表示任务处于活动状态。如果手动设置这个值，服务器会忽略修改请求。

参数	描述
条目 DN	cn=*ReplicationAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	0 | 1
默认值	
语法	整数
示例	nsDS5ReplicaReapActive: 0

2.8.27. nsDS5ReplicaRoot

此属性在复制区域的根目录中设置 DN。此属性的值必须与被复制的数据库的后缀相同，且无法修改。

参数	描述
条目 DN	cn=*ReplicationAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	要复制的数据库的后缀 - 与上面的 suffixDN 相同
默认值	
语法	DirectoryString
示例	nsDS5ReplicaRoot: "dc=example,dc=com"

2.8.28. nsDS5ReplicaSessionPauseTime

此属性设置供应商在更新会话之间应等待的时间（以秒为单位）。默认值为 0。如果属性设为负值，Directory 服务器会向客户端发送一条消息，以及 LDAP_UNWILLING_TO_PERFORM 错误代码。

nsDS5ReplicaSessionPauseTime 属性与 nsDS5ReplicaBusyWaitTime 属性一起工作。有两个属性被设计，因此 nsDS5ReplicaSessionPauseTime 间隔至少比 nsDS5ReplicaBusyWaitTime 指定的时间间隔至少一秒。较长的时间间隔可让等待供应商更好地获得消费者访问，然后以前的供应商可以重新访问消费者。

- *如果指定了任一属性，但未同时指定，则 nsDS5ReplicaSessionPauseTime 会自动设置为超过 nsDS5ReplicaBusyWaitTime 的 1 秒。*
- *如果指定了这两个属性，但 nsDS5ReplicaSessionPauseTime 小于或等于 nsDS5ReplicaBusyWaitTime，则nsDS5ReplicaSessionPauseTime 会自动设置为超过 nsDS5ReplicaBusyWaitTime。*

在设置值时，请确保 nsDS5ReplicaSessionPauseTime 间隔至少为 1 秒，超过为 nsDS5ReplicaBusyWaitTime 指定的间隔。根据需要增加间隔，直到供应商之间有可接受的消费者访问分布。

将 changetype:modify 替换为 replace 操作，随时设置 nsDS5ReplicaSessionPauseTime 属性。如果已在进行中，则更改会对下一个更新会话生效。

如果目录服务器自动重置 nsDS5ReplicaSessionPauseTime 的值，则该值只会在内部更改。对客户端看不到该更改，它不会保存到配置文件中。在外部的角度来看，属性值显示为最初设置的。

参数	描述
条目 DN	cn=*ReplicationAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	任何有效的整数
默认值	0
语法	整数
示例	nsDS5ReplicaSessionPauseTime: 0

2.8.29. nsds5ReplicaStripAttrs

部分复制允许列表从复制更新中删除的属性(nsDS5ReplicatedAttributeList)。但是，对 exclude 属性的更改仍然会触发修改事件并生成空的复制更新。

nsds5ReplicaStripAttrs 属性添加无法在空复制事件中发送的属性列表，并从更新序列中剥离。这种逻辑上包括操作 attribtes，如 modifiersName。

如果复制事件 不为空，则剥离的属性 将 被复制。只有事件为 emtpy 时，才会从更新中删除这些属性。

参数	描述
条目 DN	cn=*ReplicationAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效范围	任何支持的目录属性的以空格分隔的列表
默认值	
语法	DirectoryString
示例	nsds5ReplicaStripAttrs: modifiersname modifytimestamp

2.8.30. nsDS5ReplicatedAttributeList

此允许的属性指定 不会 复制到消费者服务器的任何属性。部分复制允许数据库在较慢的连接之间复制，或者减少安全消费者，同时仍然保护敏感信息。默认情况下，所有属性都会被复制，此属性不存在。

参数	描述
条目 DN	cn=*ReplicationAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效范围	
默认值	
语法	DirectoryString
示例	nsDS5ReplicatedAttributeList: (objectclassslackConfigs)$ EXCLUDE accountlockout memberof

2.8.31. nsDS5ReplicatedAttributeListTotal

此允许的属性指定在总更新期间没有复制到消费者服务器的任何属性。

部分复制仅复制指定的属性。这提高了整体网络性能。但是，在有些情况下，管理员可能希望在增量更新期间使用部分复制来限制某些属性，但允许在总更新期间复制这些属性（或反之亦然）。

默认情况下，所有属性都会被复制。nsDS5ReplicatedAttributeList 设置增量复制列表；如果只设置了 nsDS5ReplicatedAttributeList，则此列表也适用于总更新。

nsDS5ReplicatedAttributeListTotal 设置属性列表，使其只能从总更新中排除。

参数	描述
条目 DN	cn=*ReplicationAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效范围	
默认值	
语法	DirectoryString
示例	nsDS5ReplicatedAttributeListTotal: (objectclassPROFILE)$ EXCLUDE accountlockout

2.8.32. nsDS5ReplicaTimeout

这个允许的属性指定出站 LDAP 操作在超时和失败前等待远程副本的响应的秒数。如果服务器在错误日志文件中写入 Warning: timed out waiting 消息，则增加此属性的值。

通过检查远程计算机上的访问日志确定操作实际最后的时间，然后相应地设置 nsDS5ReplicaTimeout 属性以优化性能。

参数	描述
条目 DN	cn=*ReplicationAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效范围	0 到最大 32 位整数值(2147483647) （以秒为单位）
默认值	120
语法	整数
示例	nsDS5ReplicaTimeout: 120

2.8.33. nsDS5ReplicaTransportInfo

此属性设置用于将数据传输到副本或从副本传输数据的传输类型。设定后，无法修改此属性。

属性采用以下值：

- **STARTTLS** ：连接使用 StartTLS 命令加密。
- **LDAPS** ：连接使用 TLS 加密。
- **LDAP** ：连接使用未加密的 LDAP 协议。如果没有设置 nsDS5ReplicaTransportInfo 属性，则使用这个值。

参数	描述

参数	描述
条目 DN	cn=*ReplicationAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	StartTLS | LDAPS | LDAP
默认值	absent
语法	DirectoryString
示例	nsDS5ReplicaTransportInfo: StartTLS

2.8.34. nsDS5ReplicaUpdateInProgress

这个只读属性指出复制更新是否正在进行中。

参数	描述
条目 DN	cn=*ReplicationAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	true | false
默认值	
语法	DirectoryString
示例	nsDS5ReplicaUpdateInProgress: true

2.8.35. nsDS5ReplicaUpdateSchedule

此多值属性指定复制调度并可以被修改。对此属性所做的更改会立即生效。修改此值对暂停复制并稍后恢复非常有用。例如，如果这个值为 0000-0001 0，则无效会导致服务器停止为此复制协议发送更新。服务器将继续存储它们，以便稍后重新执行。如果该值稍后更改为 0000-2359 0123456，这将使复制立即恢复并发送所有待处理的更改。

参数	描述
条目 DN	cn=*ReplicationAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config

参数	描述
有效范围	显示的时间调度为 *XXXX-YYYY 0123456*，其中 *XXXX* 是起始小时，*YYYY* 是完成小时，数字 *0123456* 是星期几开始的天数。
默认值	0000-2359 0123456 （所有时间）
语法	整数
示例	nsDS5ReplicaUpdateSchedule: 0000-2359 0123456

2.8.36. nsDS5ReplicaWaitForAsyncResults

*在复制环境中，**nsDS5ReplicaWaitForAsyncResults** 参数设置供应商在重新发送数据前等待消费者未就绪的时间（以毫秒为单位）。*

*请注意，如果您将 **参数**设置为 **0**， 则使用默认值。*

参数	描述
条目 DN	cn=*ReplicationAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效范围	0 到最大 32 位整数(2147483647)
默认值	100
语法	整数
示例	nsDS5ReplicaWaitForAsyncResults: 100

2.8.37. nsruvReplicaLastModified

*此属性包含修改副本中的条目的最新时间，并更新 **changelog**。*

2.9. CN=SYNCAGREEMENTNAME,CN=REPLICA,CN=SUFFIX_DN,CN=MAPPING TREE,CN=CONFIG

涉及同步协议的同步属性存储在 cn=syncAgreementName,cn=suffix_DN,cn=mapping tree,cn=config 下。cn=syncAgreementName 条目是 nsDSWindowsReplicationAgreement 对象类的实例。

对于服务器要考虑的同步协议配置属性，该条目中必须存在此对象类（除 顶级 对象类之外）。同步协议仅在启用与 Windows Active Directory 服务器同步的数据库上配置。

表 2.6. 复制和同步协议间共享的属性列表

cn	nsDS5ReplicaLastUpdateEnd
description	nsDS5ReplicaLastUpdateStart
nsDS5ReplicaBindDN (Windows 同步管理器 ID)	nsDS5ReplicaLastUpdateStatus
nsDS5ReplicaBindMethod	nsDS5ReplicaPort
nsDS5ReplicaBusyWaitTime	nsDS5ReplicaRoot
nsDS5ReplicaChangesSentSinceStartup	nsDS5ReplicaSessionPauseTime
nsDS5ReplicaCredentials (Windows 同步管理器密码)	nsDS5ReplicaTimeout
nsDS5ReplicaHost (Windows 主机)	nsDS5ReplicaTransportInfo
nsDS5ReplicaLastInitEnd	nsDS5ReplicaUpdateInProgress
nsDS5ReplicaLastInitStart	nsDS5ReplicaUpdateSchedule
nsDS5ReplicaLastInitStatus	nsDS50ruv
winSyncMoveAction	winSyncInterval
nsds5ReplicaStripAttrs	

2.9.1. nsds7DirectoryReplicaSubtree

正在同步的目录服务器子树的后缀或 DN。

参数	描述
条目 DN	cn=*syncAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config

参数	描述
有效值	任何有效的后缀或子后缀
默认值	
语法	DirectoryString
示例	nsDS7DirectoryReplicaSubtree: ou=People,dc=example,dc=com

2.9.2. nsds7DirsyncCookie

这个字符串由 Active Directory DirSync 创建，并在最后一次同步时提供 Active Directory 服务器的状态。旧的 cookie 会发送到带有每个目录服务器更新的 Active Directory；新的 Cookie 与 Windows 目录数据一起返回。这意味着，仅检索自上次同步后更改的条目。

参数	描述
条目 DN	cn=*syncAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	任何字符串
默认值	
语法	DirectoryString
示例	nsDS7DirsyncCookie::khDKJFBZsjBDSCkjsdhIU74DJJVBXDhfvjmfvbhzxj

2.9.3. nsds7NewWinGroupSyncEnabled

此属性通过在 Directory Server 上创建新组来设置在 Windows 同步对等点中创建的新组是否自动同步。

参数	描述
条目 DN	cn=*syncAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	on | off

参数	描述
默认值	
语法	DirectoryString
示例	nsDS7NewWinGroupSyncEnabled: on

2.9.4. nsds7NewWinUserSyncEnabled

此属性通过在 Directory Server 上创建新条目来设置在 Windows 同步对等点中创建的新条目是否自动同步。

参数	描述
条目 DN	cn=*syncAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	on | off
默认值	
语法	DirectoryString
示例	nsDS7NewWinUserSyncEnabled: on

2.9.5. nsds7WindowsDomain

此属性设置 Windows 同步对等点所属的 Windows 域名。

参数	描述
条目 DN	cn=*syncAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	任何有效的域名
默认值	
语法	DirectoryString
示例	nsDS7WinndowsDomain: DOMAINWORLD

2.9.6. nsds7WindowsReplicaSubtree

要同步的 Windows 子树的后缀或 DN。

参数	描述
条目 DN	cn=*syncAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	任何有效的后缀或子后缀
默认值	
语法	DirectoryString
示例	nsDS7WindowsReplicaSubtree: cn=Users,dc=domain,dc=com

2.9.7. oneWaySync

此属性设定执行同步的方向。这可以从 Active Directory 服务器到目录服务器，或者从 Directory Server 到 Active Directory 服务器。

如果此属性不存在（默认），则同步协议为 双向，因此两个域中所做的更改都会被同步。

参数	描述
条目 DN	cn=*syncAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	toWindows | fromWindows | null
默认值	
语法	DirectoryString
示例	oneWaySync: fromWindows

2.9.8. winSyncInterval

此属性设置目录服务器轮询 Windows 同步对等点以查找 Active Directory 条目中的更改的频率（以秒为单位）。如果没有设置此条目，Directory 服务器会每 5 分钟检查 Windows 服务器，这意味着默认

值为 300 (300 秒)。

如果目录搜索用时过长，可以设置这个值来更快地将 Active Directory 更改写入目录服务器。

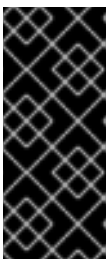
参数	描述
条目 DN	cn=*syncAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	1 到最大 32 位整数值(2147483647)
默认值	300
语法	整数
示例	winSyncInterval: 600

2.9.9. winSyncMoveAction

同步过程从根 DN 开始，开始评估条目以进行同步。条目会根据 Active Directory 中的 samAccount 和 Directory Server 中的 uid 属性关联。如果之前同步的条目（基于 samAccount/uid 关系）已从同步子树中删除，则同步插件会因为被删除或移动而从同步的子树中删除，则同步插件会识别条目不再同步。

同步协议的 winSyncMoveAction 属性设置如何处理这些移动条目的说明：

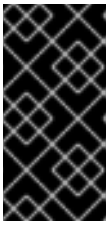
- none 不执行任何操作，因此如果存在同步的 Directory Server 条目，则它可能会在 范围内同步到或创建 Active Directory 条目。如果没有同步的 Directory Server 条目，则不会发生任何内容（这是默认行为）。
- unsync 从 Directory Server 条目中删除任何与同步相关的属性(ntUser 或 ntGroup)，但其他情况下会使 Directory Server 条目保持不变。Active Directory 和 Directory Server 条目存在于 tandem 中。



重要

稍后可能会删除不同步条目时存在风险，并且 Directory Server 条目将保持不变。这可能会造成数据不一致的问题，特别是在 Directory Server 条目稍后用于重新创建条目时。

- ***Delete 删除 Directory Server 端的对应条目，无论它是否与 Active Directory 同步（这是 9.0 中的默认行为）。***



重要

您几乎不希望删除目录服务器条目，而不删除对应的 Active Directory 条目。这个选项仅适用于与 Directory Server 9.0 系统兼容。

参数	描述
条目 DN	cn=*syncAgreementName*,cn=replica,cn=*suffixDN*,cn=mapping tree,cn=config
有效值	none | delete | unsync
默认值	none
语法	DirectoryString
示例	winSyncMoveAction: unsync

2.10. CN=REPLICATION,CN=CONFIG

此条目没有属性。在配置旧复制时，这些条目存储在 cn=replication,cn=replication 节点下，充当占位符。

2.11. CN=SASL,CN=CONFIG

包含 SASL 映射配置的条目存储在 cn=mapping,cn=sasl,cn=config 下。cn=sasl 条目是 nsContainer 对象类的实例。每个映射都是 nsSaslMapping 对象类的实例。

2.11.1. nsSaslMapBaseDNTemplate

此属性包含 SASL 身份映射中使用的搜索基本 DN 模板。

参数	描述
条目 DN	cn=*mapping_name*,cn=mapping,cn=sasl,cn=config

参数	描述
有效值	任何有效的 DN
默认值	
语法	IA5String
示例	nsSaslMapBaseDNTemplate: ou=People,dc=example,dc=com

2.11.2. nsSaslMapFilterTemplate

此属性包含 SASL 身份映射中使用的搜索过滤器模板。

参数	描述
条目 DN	cn=*mapping_name*,cn=mapping,cn=sasl,cn=config
有效值	任何字符串
默认值	
语法	IA5String
示例	nsSaslMapFilterTemplate: (cn=\1)

2.11.3. nsSaslMapPriority

目录服务器允许您设置多个简单身份验证和安全层(SASL)映射。如果 nsslapd-sasl-mapping-fallback 参数启用了 SASL 回退，您可以设置 nsSaslMapPriority 属性来优先选择单个 SASL 映射。

此设置不需要重启服务器才能生效。

参数	描述
条目 DN	cn=*mapping_name*,cn=mapping,cn=sasl,cn=config
有效值	1（最高优先级）- 100 （最低优先级）
默认值	100

参数	描述
语法	整数
示例	nsSaslMapPriority: 100

2.11.4. nsSaslMapRegexString

此属性包含用于映射 SASL 身份字符串的正则表达式。

参数	描述
条目 DN	cn=*mapping_name*,cn=mapping,cn=sasl,cn=config
有效值	任何有效的正则表达式
默认值	
语法	IA5String
示例	nsSaslMapRegexString: \(.*\)

2.12. CN=SNMP,CN=CONFIG

SNMP 配置属性存储在 cn=SNMP,cn=config 下。cn=SNMP 条目是 nsSNMP 对象类的实例。

2.12.1. nssnmpcontact

此属性设置负责维护目录服务器的人员的电子邮件地址。

参数	描述
条目 DN	cn=SNMP,cn=config
有效值	联系电子邮件地址
默认值	
语法	DirectoryString

参数	描述
示例	nssnmpcontact: jerome@example.com

2.12.2. nssnmpdescription

提供 Directory 服务器实例的唯一描述。

参数	描述
条目 DN	cn=SNMP,cn=config
有效值	描述
默认值	
语法	DirectoryString
示例	nssnmpdescription: Employee 目录实例

2.12.3. nssnmpenabled

此属性设定是否启用了 SNMP。

参数	描述
条目 DN	cn=SNMP,cn=config
有效值	on | off
默认值	on
语法	DirectoryString
示例	nssnmpenabled: off

2.12.4. nssnmplocation

此属性设置目录服务器所在的公司或机构中的位置。

参数	描述
条目 DN	cn=SNMP,cn=config
有效值	位置
默认值	
语法	DirectoryString
示例	nssnmplocation: B14

2.12.5. nssnmpmasterhost

nssnmpmasterhost 已被弃用。在引入 net-snmp 时，此属性已弃用。属性仍然会出现在 dse.ldif 中，但没有默认值。

参数	描述
条目 DN	cn=SNMP,cn=config
有效值	机器主机名或 localhost
默认值	<blank>
语法	DirectoryString
示例	nssnmpmasterhost: localhost

2.12.6. nssnmpmasterport

在引入 net-snmp 时，nssnmpmaster port 属性已弃用。属性仍然会出现在 dse.ldif 中，但没有默认值。

参数	描述
条目 DN	cn=SNMP,cn=config
有效值	操作系统依赖端口号。如需更多信息，请参阅操作系统文档。
默认值	<blank>

参数	描述
语法	整数
示例	nssnmpmasterport: 199

2.12.7. nssnmporganization

此属性设置目录服务器所属的机构。

参数	描述
条目 DN	cn=SNMP,cn=config
有效值	机构名称
默认值	
语法	DirectoryString
示例	nssnmporganization: Red Hat, Inc.

2.12.8. SNMP 统计属性

下表包含 cn=monitoring 中的只读属性，它列出了 LDAP 和 SNMP 客户端可用的统计信息。除非另有说明，否则给定属性的值是服务器收到的请求数量，或者服务器自启动以来返回的结果数。其中一些属性不适用于目录服务器，但仍需要 SNMP 客户端存在。

如果 cn=config 中的 nsslapd-counters 属性设为 on （默认设置），则 Directory 服务器实例会递增使用 64 位整数，即使 32 位机器或 32 位目录服务器版本为 32 位。所有 SNMP 统计属性都使用 64 位整数（如果已配置）。

注意

nsslapd-counters 属性为这些特定的数据库和服务器计数器启用 64 位整数。使用 64 位整数的计数器不可配置；所有允许的计数器都启用了 64 位整数，或为所有允许的计数器禁用。

表 2.7. SNMP Statistic 属性

属性	描述
AnonymousBinds	这显示了匿名绑定请求数。
UnAuthBinds	这显示了未经身份验证的（匿名）绑定的数量。
SimpleAuthBinds	这显示了 LDAP 简单绑定请求(DN 和密码)的数量。
StrongAuthBinds	这显示了所有 SASL 机制的 LDAP SASL 绑定请求数量。
BindSecurityErrors	这显示了在绑定请求中给出无效密码的次数。
InOps	这将显示服务器接收的所有请求的总数。
ReadOps	未使用。这个值始终为 **0**。
CompareOps	这显示了 LDAP 比较请求的数量。
AddEntryOps	这显示了 LDAP 添加请求的数量。
RemoveEntryOps	这显示了 LDAP 删除请求的数量。
ModifyEntryOps	这显示了 LDAP 修改请求的数量。
ModifyRDNOps	这显示了 LDAP 修改 RDN (modrdn)请求的数量。
ListOps	未使用。这个值始终为 **0**。
SearchOps	这将显示 LDAP 搜索请求的数量。
OneLevelSearchOps	这显示了单级搜索操作的数量。
WholeSubtreeSearchOps	这显示了子树级搜索操作的数量。
引用	这显示了返回的 LDAP 引用的数量。
链	未使用。这个值始终为 **0**。
SecurityErrors	这显示了返回的安全相关错误数量，如无效的密码、未知或无效的身份验证方法，或者所需的更强大的身份验证。
错误	这将显示返回的错误数量。
连接	这显示了当前打开的连接的数量。

属性	描述
ConnectionSeq	这将显示打开的连接总数，包括当前打开的连接和关闭的连接。
BytesRecv	这显示了收到的字节数。
BytesSent	这将显示发送的字节数。
EntriesReturned	这将显示返回为搜索结果的条目数量。
ReferralsReturned	这提供了关于返回搜索结果的信息（持续引用引用）。
MasterEntries	未使用。这个值始终为 **0**。
CopyEntries	未使用。这个值始终为 **0**。
CacheEntries[a]	如果服务器只有一个数据库后端，这是在条目缓存中缓存的条目数。如果服务器有多个数据库后端，则这个值为 **0**， 并且查看每个数据库的 monitor 条目以了解更多信息。
CacheHits	如果服务器只有一个数据库后端，这是从条目缓存返回的条目数，而不是从数据库返回的条目数，用于搜索结果。如果服务器有多个数据库后端，则这个值为 **0**， 并且查看每个数据库的 monitor 条目以了解更多信息。
SlaveHits	未使用。这个值始终为 **0**。
[a] **CacheEntries** 和 **CacheHits** 每 10 (10)秒更新一次。红帽强烈建议使用这个数据库后端和其他数据库信息的特定监控条目。	

2.13. CN=UNIQUEID GENERATOR,CN=CONFIG

唯一的 ID 生成器配置属性存储在 cn=uniqueid generator,cn=config 下。cn=uniqueid generator 条目是一个 scalable Object 对象类的实例。

2.13.1. nsstate

此属性在服务器重启后保存唯一 ID 生成器的状态。此属性由服务器维护。不要编辑它。

参数	描述
条目 DN	cn=uniqueid generator,cn=config
有效值	
默认值	
语法	DirectoryString
示例	nsstate: AbId0c3oMIDUntiLCyYNGgAAAAAAAAAA

2.14. CN=TASKS,CN=CONFIG 下条目的通用任务调用属性

一些核心目录服务器，可以使用 LDAP 工具编辑目录条目来启动任务。这些任务条目包含在 cn=tasks,cn=config 中。可以通过更新条目来调用每个任务，例如：

```
dn: cn=task_id,cn=task_type,cn=tasks,cn=config
...
```

本节列出了所有任务类型的通用属性。

重要

任务条目不是永久配置条目。它们仅在任务操作正在运行或直到 ttl 周期过期时才存在于配置文件中。然后，服务器自动删除该条目。

2.14.1. cn

cn 属性标识要启动的新任务操作。cn 属性值可以是任意的，只要它定义了新任务。

参数	描述
条目 DN	cn=*task_name*,cn=*task_type*,cn=tasks,cn=config
有效值	任何字符串
默认值	
语法	DirectoryString

参数	描述
示例	cn: example task entry name

2.14.2. nsTaskCancel

此属性允许在进行过程中中止任务。此属性可以被用户修改。

参数	描述
条目 DN	cn=*task_name*,cn=*task_type*,cn=tasks,cn=config
有效值	true | false
默认值	
语法	不区分大小写的字符串
示例	nsTaskCancel: true

2.14.3. nsTaskCurrentItem

此属性显示任务操作完成的子任务数量，假设任务可以分为子任务。如果只有一个任务，则 nsTaskCurrentItem 在任务运行时为 0，在任务完成后为 1。这样，属性与进度条类似。当 nsTaskCurrentItem 属性的值与 nsTaskTotalItems 相同时，任务已完成。

此属性值由服务器设置，不应 编辑。

参数	描述
条目 DN	cn=*task_name*,cn=*task_type*,cn=tasks,cn=config
有效值	0 到最大 32 位整数值(2147483647)
默认值	
语法	整数
示例	nsTaskCurrentItem: 148

2.14.4. nsTaskExitCode

此属性包含任务的退出代码。此属性仅在任务完成后存在，且任何值仅在任务完成后有效。结果代码可以是任何 LDAP 退出代码，但只有 0 值等于成功；任何其他结果代码都是错误。

此属性值由服务器设置，不应 编辑。

参数	描述
条目 DN	cn=*task_name*,cn=*task_type*,cn=tasks,cn=config
有效值	0 （成功）到 97[a]
默认值	
语法	整数
示例	nsTaskExitCode: 0
[a] **0** 以外的任何响应都是一个错误。	

2.14.5. nsTaskLog

此条目包含任务的所有日志消息，包括警告和信息消息。新消息会附加到条目值的末尾，因此此属性值会增大，而不默认删除原始内容。

成功的任务操作(nsTaskExitCode 为 0) 仅在 nsTaskLog 属性中记录。任何非零响应（表示错误）都可以记录为错误，但错误消息仅记录在 nsTaskLog 属性中。因此，使用 nsTaskLog 属性中的信息来查找发生哪些错误。

此属性值由服务器设置，不应 编辑。

2.14.6. nsTaskStatus

此属性包含有关任务状态的更改信息，如累积统计数据或其当前输出消息。只要进程正在运行，属性的整个内容可能会定期更新。

此属性值由服务器设置，不应 编辑。

参数	描述
条目 DN	cn=*task_name*,cn=*task_type*,cn=tasks,cn=config
有效值	任何字符串
默认值	
语法	case-exact 字符串
示例	nsTaskStatus: Loading entries....

2.14.7. nsTaskTotalItems

此属性显示必须为任务操作完成的子任务总数。当 nsTaskCurrentItem 属性的值与 nsTaskTotalItems 相同时，任务已完成。

此属性值由服务器设置，不应 编辑。

参数	描述
条目 DN	cn=*task_name*,cn=*task_type*,cn=tasks,cn=config
有效值	0 到最大 32 位整数值(2147483647)
默认值	
语法	整数
示例	nsTaskTotalItems: 152

2.14.8. ttl

此属性设置任务条目在任务完成或中止后仍保留在 DSE 的时间（以秒为单位）。设置 ttl 属性允许针对新状态信息轮询任务条目，而不缺少退出代码。将 ttl 属性设置为 0 表示该条目不会被缓存。

参数	描述
条目 DN	cn=*task_name*,cn=*task_type*,cn=tasks,cn=config
有效值	0 （不能缓存）到最大 32 位整数值(2147483647)

参数	描述
默认值	
语法	DirectoryString
示例	ttl: 120

2.15. CN=TASK_NAME,CN=IMPORT,CN=TASKS,CN=CONFIG

LDIF 文件或多个 LDIF 文件可以通过命令行导入，方法是创建一个特殊任务条目来定义任务的参数并启动任务。任务完成后，任务条目会从目录中删除。

cn=import 条目是导入任务操作的容器条目。cn=import 条目本身没有属性，但此条目中的每个任务条目（如 cn=task_name,cn=import,cn=tasks,cn=config ）都使用以下属性来定义导入任务。

cn=import 下的导入任务条目必须包含要导入的 LDIF 文件（在 nsFilename 属性中）以及要导入该文件的实例名称（在 nsInstance 属性中）。另外，它必须包含一个唯一的 cn 来识别该任务。例如：

```
dn: cn=example import,cn=import,cn=tasks,cn=config
objectclass: extensibleObject
cn: example import
nsFilename: /home/files/example.ldif
nsInstance: userRoot
```

当导入操作运行时，任务条目将包含 cn=tasks,cn=config 下的 Common task invocation 属性中列出的所有服务器生成的任务属性。

2.15.1. nsExcludeSuffix

此属性标识 LDIF 文件中的后缀或子树，以便从导入中排除。

参数	描述
条目 DN	cn=*task_name*,cn=import,cn=tasks,cn=config
有效值	任何 DN
默认值	

参数	描述
语法	DN、多值
示例	nsExcludeSuffix: ou=machines,dc=example,dc=com

2.15.2. nsFilename

nsFilename 属性包含要导入到目录服务器实例的 LDIF 文件的路径和文件名。要导入多个文件，请添加此属性的多个实例。例如：

```
nsFilename: file1.ldif
nsFilename: file2.ldif
```

参数	描述
条目 DN	cn=*task_name*,cn=import,cn=tasks,cn=config
有效值	任何字符串
默认值	
语法	case-exact 字符串，多值
示例	nsFilename: /home/jsmith/example.ldif

2.15.3. nsImportChunkSize

此属性定义导入操作期间具有的块数量，这会在导入时覆盖服务器在启动新传递并合并块时的检测。

参数	描述
条目 DN	cn=*task_name*,cn=import,cn=tasks,cn=config
有效值	0 到最大 32 位整数值(2147483647)
默认值	0
语法	整数
示例	nsImportChunkSize: 10

2.15.4. nsImportIndexAttrs

此属性设定是否索引导入到数据库实例中的属性。

参数	描述
条目 DN	cn=*task_name*,cn=import,cn=tasks,cn=config
有效值	true | false
默认值	true
语法	不区分大小写的字符串
示例	nsImportIndexAttrs: true

2.15.5. nsIncludeSuffix

此属性标识要从 LDIF 文件导入的特定后缀或子树。

参数	描述
条目 DN	cn=*task_name*,cn=import,cn=tasks,cn=config
有效值	任何 DN
默认值	
语法	DN、多值
示例	nsIncludeSuffix: ou=people,dc=example,dc=com

2.15.6. nsInstance

此属性提供要导入文件的数据库实例的名称，如 userRoot 或 slapd-示例。

参数	描述
条目 DN	cn=*task_name*,cn=import,cn=tasks,cn=config
有效值	目录服务器实例数据库的名称（任何字符串）

参数	描述
默认值	
语法	case-exact 字符串
示例	nsInstance: userRoot

2.15.7. nsUniqueIdGenerator

此属性定义如何生成基于名称的 ID；属性设置要用来生成 ID 的命名空间。当条目需要有相同的 ID 时，此选项可用于将同一 LDIF 文件导入到两个目录服务器实例中。

参数	描述
条目 DN	cn=*task_name*,cn=import,cn=tasks,cn=config
有效值	任何字符串
默认值	
语法	不区分大小写的字符串
示例	nsUniqueIdGeneratorNamespace: example

2.15.8. nsUniqueIdGeneratorNamespace

此属性定义如何生成基于名称的 ID；属性设置要用来生成 ID 的命名空间。当条目需要有相同的 ID 时，此选项可用于将同一 LDIF 文件导入到两个目录服务器实例中。

参数	描述
条目 DN	cn=*task_name*,cn=import,cn=tasks,cn=config
有效值	任何字符串
默认值	
语法	不区分大小写的字符串
示例	nsUniqueIdGeneratorNamespace: example

2.16. CN=TASK_NAME,CN=EXPORT,CN=TASKS,CN=CONFIG

可以通过命令行导出数据库或多个数据库，该条目定义任务的参数并启动该任务。任务完成后，任务条目会从目录中删除。

cn=export,cn=tasks,cn=config 条目是用于导出任务操作的容器。这些任务存储在此容器中，并命名为 cn=task_name,cn=export,cn=tasks,cn=config。

在导出操作运行时，任务条目包含 cn=tasks,cn=config 下的 Common task invocation 属性中列出的所有服务器生成的任务属性。

2.16.1. nsDumpUniqId

此属性设置导出条目的唯一 ID 不会导出。

参数	描述
条目 DN	cn=*task_name*,cn=export,cn=tasks,cn=config
有效值	true | false
默认值	true
语法	不区分大小写的字符串
示例	nsDumpUniqId: true

2.16.2. nsExcludeSuffix

此属性标识数据库中要从导出的 LDIF 文件中排除的后缀或子树。

参数	描述
条目 DN	cn=*task_name*,cn=export,cn=tasks,cn=config
有效值	任何 DN
默认值	

参数	描述
语法	DN、多值
示例	nsExcludeSuffix: ou=machines,dc=example,dc=com

2.16.3. nsExportReplica

此属性标识是否要在复制中使用导出的数据库。对于副本，正确的属性和设置将包含在条目中，以自动初始化副本。

参数	描述
条目 DN	cn=*task_name*,cn=export,cn=tasks,cn=config
有效值	true | false
默认值	false
语法	不区分大小写的字符串
示例	nsExportReplica: true

2.16.4. nsFilename

nsFilename 属性包含 LDIF 文件的路径和文件名，以将 Directory Server 实例数据库导出到其中。

参数	描述
条目 DN	cn=*task_name*,cn=export,cn=tasks,cn=config
有效值	任何字符串
默认值	
语法	case-exact 字符串，多值
示例	nsFilename: /home/jsmith/example.ldif

2.16.5. nsIncludeSuffix

此属性标识要导出到 LDIF 文件的特定后缀或子树。

参数	描述
条目 DN	cn=*task_name*,cn=export,cn=tasks,cn=config
有效值	任何 DN
默认值	
语法	DN、多值
示例	nsIncludeSuffix: ou=people,dc=example,dc=com

2.16.6. nsInstance

此属性提供从中导出数据库的数据库实例的名称，如 userRoot 或 userRoot。

参数	描述
条目 DN	cn=*task_name*,cn=export,cn=tasks,cn=config
有效值	目录服务器实例（任何字符串）的名称
默认值	
语法	case-exact 字符串，多值
示例	nsInstance: userRoot

2.16.7. nsNoWrap

此属性设置是否在 LDIF 文件中嵌套长行。

参数	描述
条目 DN	cn=*task_name*,cn=export,cn=tasks,cn=config
有效值	true | false
默认值	false

参数	描述
语法	不区分大小写的字符串
示例	nsNoWrap: false

2.16.8. nsPrintKey

此属性设定在导出任务处理条目时是否打印条目 ID 号。

参数	描述
条目 DN	cn=*task_name*,cn=export,cn=tasks,cn=config
有效值	true | false
默认值	true
语法	不区分大小写的字符串
示例	nsPrintKey: false

2.16.9. nsUseId2Entry

nsUseId2Entry 属性使用主数据库索引 id2entry 来定义导出的 LDIF 条目。

参数	描述
条目 DN	cn=*task_name*,cn=export,cn=tasks,cn=config
有效值	true | false
默认值	false
语法	不区分大小写的字符串
示例	nsUseId2Entry: true

2.16.10. nsUseOneFile

此属性设定是否将所有目录服务器实例导出到单个 LDIF 文件或单独的 LDIF 文件。

参数	描述
条目 DN	cn=*task_name*,cn=export,cn=tasks,cn=config
有效值	true | false
默认值	true
语法	不区分大小写的字符串
示例	nsUseOneFile: true

2.17. CN=TASK_NAME,CN=BACKUP,CN=TASKS,CN=CONFIG

可以通过命令行备份数据库，方法是创建一个特殊的任务条目来定义任务的参数并启动任务。任务完成后，任务条目会从目录中删除。

cn=backup 条目是备份任务操作的容器条目。cn=backup 条目本身没有属性，但此条目中的每个任务条目（如 cn='task_ID,cn=backup,cn=tasks,cn=config ）都使用以下属性来定义备份任务。

cn=backup 下的备份任务条目必须包含要复制存档副本的目录位置（在 backup-nsArchiveDir 属性中）以及要备份的数据库类型（在 backup-nsDatabaseType' 属性中）。另外，它必须包含一个唯一的 cn 来识别该任务。例如：

```
dn: cn=example backup,cn=backup,cn=tasks,cn=config
objectclass: extensibleObject
cn: example backup
nsArchiveDir: /export/backups/_ nsDatabaseType: ldbm database__
```

当备份操作运行时，任务条目将包含 cn=tasks,cn=config 下的 Common task invocation 属性中列出的所有服务器生成的任务属性。

2.17.1. nsArchiveDir

此属性提供要写入备份的目录的位置。

此处的备份目录通常与 nsslapd-bakdir 属性中配置的目录相同。

如果 cn=backup 任务中没有包含此属性，则任务将失败，并显示 LDAP 对象类违反错误(65)。

参数	描述
条目 DN	cn=*task_name*,cn=backup,cn=tasks,cn=config
有效值	任何本地目录位置
默认值	
语法	case-exact 字符串
示例	nsArchiveDir: /export/backups

2.17.2. nsDatabaseType

此属性提供正在存档的数据库类型。设置数据库类型信号了备份插件目录服务器应使用什么类型来归档数据库。

参数	描述
条目 DN	cn=*task_name*,cn=backup,cn=tasks,cn=config
有效值	ldbm 数据库
默认值	ldbm 数据库
语法	case-exact 字符串
示例	nsDatabaseType: ldbm database

2.18. CN=TASK_NAME,CN=RESTORE,CN=TASKS,CN=CONFIG

可以通过命令行恢复数据库，该条目定义任务的参数并启动任务。任务完成后，任务条目会从目录中删除。

cn=restore 条目是一个容器条目，用于任务操作来恢复数据库。cn=restore 条目本身没有属性，但此条目中的每个任务条目（如 cn=task_ID,cn=restore,cn=tasks,cn=config ）都使用以下属性来定义恢复

任务。

cn=restore 下的恢复任务条目必须包含检索存档副本的目录位置（在 restore-nsArchiveDir 属性中）以及要恢复的数据库类型（在 restore-nsDatabaseType 属性中）。另外，它必须包含一个唯一的 cn 来识别该任务。例如：

```
dn: cn=example restore,cn=restore,cn=tasks,cn=config
objectclass: extensibleObject
cn: example restore
nsArchiveDir: /export/backups/
nsDatabaseType: ldbm database
```

当恢复操作运行时，任务条目将包含 cn=tasks,cn=config 下的 Common task invocation 属性中列出的所有服务器生成的任务属性。

2.18.1. nsArchiveDir

此属性提供要写入备份的目录的位置。

参数	描述
条目 DN	cn=*task_name*,cn=restore,cn=tasks,cn=config
有效值	任何本地目录位置
默认值	
语法	case-exact 字符串
示例	nsArchiveDir: /export/backups

2.18.2. nsDatabaseType

此属性提供正在存档的数据库类型。设置数据库类型信号了备份插件目录服务器应使用什么类型来归档数据库。

参数	描述
条目 DN	cn=*task_name*,cn=restore,cn=tasks,cn=config
有效值	ldbm 数据库

参数	描述
默认值	ldbm 数据库
语法	case-exact 字符串
示例	nsDatabaseType: ldbm database

2.19. CN=TASK_NAME,CN=INDEX,CN=TASKS,CN=CONFIG

可以通过命令行来索引目录属性，方法是创建一个特殊任务条目来定义任务的参数并启动任务。任务完成后，任务条目会从目录中删除。

cn=index 条目是索引任务操作的容器条目。cn=index 条目本身没有属性，但此条目中的每个任务条目（如 cn=task_ID,cn=index,cn=tasks,cn=config ）都使用以下属性来定义备份任务。

cn=index 下的索引任务条目可以通过标识要索引的属性和要创建的索引类型（在 nsIndexAttribute 属性中定义）来创建标准索引。

或者，可使用 nsIndexVLVAttribute 属性为属性生成虚拟列表视图(VLV)索引。这与运行 vlvindex 脚本相同。

例如：

```
dn: cn=example presence index,cn=index,cn=tasks,cn=config
objectclass: top
objectclass: extensibleObject
cn: example presence index
nsInstance: userRoot
nsIndexAttribute: cn:pres

dn: cn=example VLV index,cn=index,cn=tasks,cn=config
objectclass: extensibleObject
cn: example VLV index
nsIndexVLVAttribute: "by MCC ou=people,dc=example,dc=com"
```

当索引操作运行时，任务条目将包含 cn=tasks,cn=config 下的 Common task invocation 属性中列出的所有服务器生成的任务属性。

2.19.1. nsIndexAttribute

此属性提供要索引和要应用的索引类型的属性名称。属性值的格式是属性名称和以逗号分隔的索引类型列表，用双引号括起来。例如：

```
nsIndexAttribute: attribute:index1,index2
```

参数	描述
条目 DN	cn=*task_name*,cn=index,cn=tasks,cn=config
有效值	* 任何属性 * 索引类型，可以是 **pres** (presence), **eq** (equality), **approx** (approximate)和 **sub** （子字符串）
默认值	
语法	不区分大小写的字符串，多值
示例	* nsIndexAttribute: cn:pres,eq * nsIndexAttribute: description:sub

2.19.2. nsIndexVLVAttribute

此属性提供 VLV 索引的目标条目的名称。虚拟列表视图基于浏览索引条目，用于定义虚拟列表基本 DN、范围和过滤器。nsIndexVLVAttribute 值是浏览索引条目，VLV 创建任务会根据浏览索引条目参数运行。

参数	描述
条目 DN	cn=*task_name*,cn=index,cn=tasks,cn=config
有效值	VLV 条目定义的子条目 RDN
默认值	
语法	DirectoryString
示例	nsIndexVLVAttribute: "*浏览索引排序标识符*"

2.20. CN=TASK_NAME,CN=SCHEMA RELOAD TASK,CN=TASKS,CN=CONFIG

当目录实例启动或重启时，目录模式会被加载。对目录架构的任何更改（包括添加自定义架构元素）都

不会自动加载并可供实例使用，直到服务器重新启动或启动架构重新加载任务为止。

可以动态重新加载自定义架构更改，而无需重启 Directory 服务器实例。这可以通过在 cn=tasks 条目下创建新任务条目来启动 schema reload 任务。

自定义架构文件可以位于任何目录中；如果没有通过 schemadir 属性指定，服务器会从默认的 /etc/dirsrv/slapd-instance_name/schema/ 目录中重新载入 schema。

重要

从另一个目录加载的任何模式都必须复制到 schema 目录中，或者服务器时模式将会丢失。

架构重新加载任务通过命令行启动，方法是创建一个特殊任务条目来定义任务的参数并启动任务。任务完成后，任务条目会从目录中删除。例如：

```
dn: cn=example schema reload,cn=schema reload task,cn=tasks,cn=config
objectclass: extensibleObject
cn:example schema reload
schemadir: /export/schema
```

cn=schema reload 任务 条目是 schema reload 操作的容器条目。cn=schema reload 任务 条目本身没有属性，但此条目中的每个任务条目（如 cn='task_ID,cn=schema reload 任务,cn=tasks,cn=config ）使用 schema reload 属性来定义单独的重新加载任务。

2.20.1. cn

cn 属性标识要启动的新任务操作。cn 属性值可以是任意的，只要它定义了新任务。

参数	描述
条目 DN	cn=*task_name*,cn=schema reload task,cn=tasks,cn=config
有效值	任何字符串
默认值	
语法	DirectoryString

参数	描述
示例	cn: example reload 任务 ID

2.20.2. schemadir

这包括包含自定义模式文件的目录的完整路径。

参数	描述
条目 DN	cn=*task_name*,cn=schema reload task,cn=tasks,cn=config
有效值	任何本地目录路径
默认值	/etc/dirsrv/schema
语法	DirectoryString
示例	schemadir: /export/schema/

2.21. CN=TASK_NAME,CN=MEMBEROF TASK,CN=TASKS,CN=CONFIG

memberOf 属性由 Directory Server 创建和管理，以显示成员用户条目的组成员资格。更改组条目上的 member 属性时，所有成员的相关目录条目都会使用对应的 memberOf 属性自动更新。

cn=memberof 任务 用于在目录中成员用户条目上创建初始 memberOf 属性。创建 memberOf 属性后，MemberOf 插件会自动管理 memberOf 属性。

memberOf 更新任务必须提供条目或子树的 DN，以便针对运行更新任务（在 memberof-basdn 属性中设置）。（可选）任务可以包含一个过滤器，用于识别要更新的成员用户条目（在 memberof-filter 属性中设置）。例如：

```
dn: cn=example memberOf,cn=memberof task,cn=tasks,cn=config
objectclass: extensibleObject
cn:example memberOf
basedn: ou=people,dc=example,dc=com
filter: (objectclass=groupofnames)
```

任务完成后，任务条目会从目录中删除。

cn=memberof 任务 条目是 memberOf 更新操作的容器条目。cn=memberof 任务 条目本身没有属性，但此条目下的每个任务条目（如 cn=task_ID,cn=memberof 任务,cn=tasks,'cn=config ）使用其属性来定义单独的更新任务。

2.21.1. basedn

此属性提供用于搜索更新 memberOf 属性的用户条目的基本 DN。

参数	描述
条目 DN	cn=*task_name*,cn=memberof task,cn=tasks,cn=config
有效值	任何 DN
默认值	
语法	DN
示例	baseDN: ou=people,dc=example,dc=com

2.21.2. filter

此属性提供可选的 LDAP 过滤器，用于选择要更新 memberOf 属性的用户条目。组的每个成员在目录中都有对应的用户条目。

参数	描述
条目 DN	cn=*task_name*,cn=memberof task,cn=tasks,cn=config
有效值	任何 LDAP 过滤器
默认值	(objectclass=*)
语法	DirectoryString
示例	filter: (l=Sunnyvale)

2.22. CN=TASK_NAME,CN=FIXUP LINKED ATTRIBUTES TASK,CN=TASKS,CN=CONFIG

目录服务器具有 Linked 属性插件，它允许一个属性（在一个条目中设置）来自动更新另一个条目中的另一个属性。两个条目都具有值的 DN。第一个条目中的 DN 值指向要更新插件的条目；第二个条目中的

属性包含到第一个条目的 DN 后端程序。

这与 MemberOf 插件使用 group 条目中的 member 属性在用户条目中设置 memberOf 属性的方式类似。使用链接的属性时，任何属性都可以定义为"链接"，然后在受影响的条目中另一个属性为"managed"。

在创建 链接插件实例时，cn=fixup 链接属性会根据数据库中已存在的链接属性创建受管属性。设置链接和受管属性后，链接属性插件会动态维护受管属性，因为用户更改链接属性。

链接的属性更新任务可以指定要更新的链接属性插件实例，在可选的 cn-fixup-linked-attributes-linkdn 属性中设置。如果在任务条目上没有设置此属性，则所有配置的链接属性都会被更新。

```
dn: cn=example,cn=fixup linked attributes,cn=tasks,cn=config
objectclass: extensibleObject
cn:example
linkdn: cn=Example Link,cn=Linked Attributes,cn=plugins,cn=config
```

任务完成后，任务条目会从目录中删除。

cn=fixup 链接的属性条目是任何链接的属性更新操作的容器条目。cn=fixup 链接的属性 条目本身没有与单个任务相关的属性，但此条目下的每个任务都没有相关的属性，如 cn='task_ID,cn=fixup 链接的属性,cn=tasks,cn=config 来定义单独的更新任务。

2.22.1. linkdn

每个链接管理的属性对都在链接的属性插件实例中进行配置。linkdn 属性通过提供插件实例 DN 设置用于更新条目的特定链接属性插件。例如：

```
linkdn: cn=Manager Attributes,cn=Linked Attributes,cn=plugins,cn=config
```

如果没有提供插件实例，则会更新所有链接的属性。

参数	描述
条目 DN	cn=*task_name*,cn=fixup 链接的属性,cn=tasks,cn=config
有效值	DN （用于链接属性插件的实例）

参数	描述
默认值	无
语法	DN
示例	linkdn: cn=Manager Links,cn=Linked Attributes,cn=plugins,cn=config

2.23. CN=TASK_NAME,CN=SYNTAX VALIDATE,CN=TASKS,CN=CONFIG

语法验证会检查属性的每个修改，以确保新值具有该属性类型所需的语法。属性语法会根据 RFC 4514 中的定义进行验证。

默认启用语法验证。但是，语法验证仅审核对属性值的更改，如添加或修改属性时。它不会验证现有属性值的语法。

可以通过语法验证任务来验证现有语法。此任务检查指定子树下的条目（在 syntax-validation-basedn 属性中），并且只有与指定过滤器匹配的条目（在 syntax-validation-filter 属性中）。

```
dn: cn=example,cn=syntax validate,cn=tasks,cn=config
objectclass: extensibleObject
cn:example
basedn: ou=people,dc=example,dc=com
filter: "(objectclass=inetorgperson)"
```

任务完成后，任务条目会从目录中删除。

如果禁用了语法验证，或者服务器迁移了语法验证，那么服务器中可能会存在不符合属性语法要求的数据。可以运行语法验证任务，在启用语法验证前评估这些现有的属性值。

cn=syntax validate 条目是任何语法验证操作的容器条目。cn=syntax validate 条目本身没有特定于任何任务的属性。此条目下的每个任务条目（如 cn=task_ID,cn=syntax validate,cn=tasks,'cn=config ）都使用其属性来定义单独的更新任务。

2.23.1. basedn

提供运行语法验证任务的子树。例如：

basedn: ou=people,dc=example,dc=com

参数	描述
条目 DN	cn=*task_name*,cn=syntax validate,cn=tasks,cn=config
有效值	任何 DN
默认值	无
语法	DN
示例	basedn: dc=example,dc=com

2.23.2. filter

包含一个可选 LDAP 过滤器，可用于识别给定运行语法验证任务的给定下的特定条目。如果没有在任务上设置此属性，则对 basedn 中的每个条目都会被审核。例如：

filter: "(objectclass=person)"

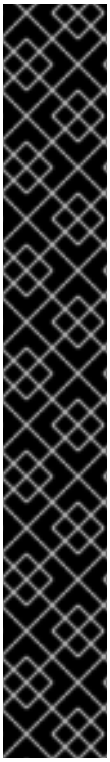
参数	描述
条目 DN	cn=*task_name*,cn=syntax validate,cn=tasks,cn=config
有效值	任何 LDAP 过滤器
默认值	"(objectclass=*)"
语法	DirectoryString
示例	filter: " (objectclasscategories) "

2.24. CN=TASK_NAME,CN=USN TOMBSTONE CLEANUP TASK,CN=TASKS,CN=CONFIG

如果启用了 USN 插件，则每当目录写入操作（如添加或修改）时，会在每个条目上设置 更新序列号 (USN)。这反映在 entryUSN 操作属性中。即使删除了条目，并且 Directory Server 实例维护 tombstone 条目，也会设置此 USN。

cn=USN tombstone cleanup 任务 根据后端数据库(在后端 属性中)或后缀（在 suffix 属性中）删除实例维护的 tombstone 条目。（可选）可以通过指定要删除的最大 USN （在 max-usn-to-delete 属性中）来删除 tombstone 条目的子集，这会保留最新的 tombstone 条目。

```
dn: cn=example,cn=USN tombstone cleanup task,cn=tasks,cn=config
objectclass: extensibleObject
cn:example
backend: userroot
max_usn_to_delete: 500
```



重要

此任务只能在未启用复制时启动。复制维护自己的 tombstone 存储，这些 tombstone 条目不能被 USN 插件删除；它们必须由复制进程维护。因此，目录服务器可防止用户为复制数据库运行清理任务。

尝试为复制后端创建此任务条目将在命令行中返回这个错误：

```
ldap_add: DSA is unwilling to perform
```

在错误日志中，存在更明确的信息，因为后缀因为被复制而没有 tombstone。

```
[...] usn-plugin - Suffix dc=example,dc=com is replicated. Unwilling to perform
cleaning up tombstones.
```

任务完成后，任务条目会从目录中删除。

cn=USN tombstone cleanup 任务 条目是所有 USN tombstone delete 操作的一个容器条目。cn=USN tombstone cleanup 任务 本身没有与任何单个任务相关的属性，但此条目下的每个任务都没有相关的属性，如 cn='task_ID,cn=USN tombstone cleanup 任务,cn=tasks,cn=config，使用其属性来定义单独的更新任务。

2.24.1. 后端

这为 Directory 服务器实例后端或数据库提供运行清理操作。如果没有指定后端，则必须指定后缀。

参数	描述
条目 DN	cn=*task_name*,cn=USN tombstone cleanup task,cn=tasks,cn=config
有效值	数据库名称

参数	描述
默认值	无
语法	DirectoryString
示例	后端：userroot

2.24.2. max_usn_to_delete

这在删除 tombstone 条目时给出最高 USN 值来删除。所有 tombstone 条目（包括该数字）都将被删除。具有较高 USN 值的 tombstone 条目（这意味着更最新的条目）不会被删除。

参数	描述
条目 DN	cn=*task_name*,cn=USN tombstone cleanup task,cn=tasks,cn=config
有效值	任何整数
默认值	无
语法	整数
示例	max_usn_to_delete: 500

2.24.3. suffix

这提供了目录服务器中的后缀或子树来运行清理操作。如果没有指定后缀，则必须为后端指定。

参数	描述
条目 DN	cn=*task_name*,cn=USN tombstone cleanup task,cn=tasks,cn=config
有效值	任何子树 DN
默认值	无
语法	DN
示例	suffix: dc=example,dc=com

2.25. CN=TASK_NAME,CN=CLEANALLRUV,CN=TASKS,CN=CONFIG

有关复制拓扑的信息 - 所有供应商都相互提供更新，同一复制组中的其他副本都包含在一组称为 副本更新向量(RUV)的元数据中。RUV 包含有关供应商 ID 和 URL 的信息，它的最新更改状态号用于本地服务器上所做的更改，以及第一次更改的 CSN。供应商和消费者均存储 RUV 信息，它们使用它来控制复制更新。

当一个供应商从复制拓扑中删除时，它可能保留在另一个副本的 RUV 中。当其他副本重启时，它会在日志中记录复制插件无法识别（删除）供应商的错误。

```
[09/Sep/2021:09:03:43 -0600] NSMMReplicationPlugin - ruv_compare_ruv: RUV [changelog
max RUV] does not
 contain element [{replica 55 ldap://server.example.com:389} 4e6a27ca000000370000
4e6a27e8000000370000]
 which is present in RUV [database RUV]
......
[09/Sep/2021:09:03:43 -0600] NSMMReplicationPlugin - replica_check_for_data_reload:
Warning: for replica
 dc=example,dc=com there were some differences between the changelog max RUV and the
database RUV.  If
 there are obsolete elements in the database RUV, you should remove them using the
CLEANRUV task.  If they
 are not obsolete, you should check their status to see why there are no changes from those
servers in the changelog.
```

当从拓扑中永久删除供应商时，任何有关该供应商的元数据都应从其它供应商的 RUV 条目中清除。

cn=cleanallruv 任务通过复制拓扑中的所有服务器传播，并删除与指定缺失或过时的供应商关联的 RUV 条目。

任务完成后，任务条目会从目录中删除。

cn=cleanallruv 条目是所有清理 RUV 操作的容器条目。cn=cleanallruv 条目本身没有与任何单个任务相关的属性，但此条目下的每个任务都没有相关的属性，如 cn=task_ID,cn=cleanallruv,cn=tasks,cn=config 来定义单个更新任务。

每个清理 RUV 任务都必须指定要删除的副本 RUV 条目的副本 ID 号、复制数据库的基于 DN，以及是否在删除 RUV 数据前应用缺少的供应商中剩余的更新。

```
dn: cn=clean 55,cn=cleanallruv,cn=tasks,cn=config
objectclass: extensibleObject
```

```
replica-base-dn: dc=example,dc=com
replica-id: 55
replica-force-cleaning: no
cn: clean 55
```

2.25.1. replica-base-dn

这提供了与复制数据库关联的目录服务器基本 DN。这是复制后缀的基本 DN。

参数	描述
条目 DN	cn=*task_name*,cn=cleanallruv,cn=tasks,cn=config
有效值	目录后缀 DN
默认值	无
语法	DirectoryString
示例	replica-base-dn: dc=example,dc=com

2.25.2. replica-force-cleaning

这将设置任何来自副本的未完成的更新是否应被应用(无)或 clean RUV 操作是否应强制持续并丢失任何剩余的更新（是 ）。

参数	描述
条目 DN	cn=*task_name*,cn=cleanallruv,cn=tasks,cn=config
有效值	No | yes
默认值	无
语法	DirectoryString
示例	replica-force-cleaning: no

2.25.3. replica-id

这提供了从复制拓扑 中删除 的副本配置条目的 nsDS5ReplicaId 属性中的副本 ID （在 nsDS5ReplicaId 属性中定义）。

参数	描述
条目 DN	cn=*task_name*,cn=cleanallruv,cn=tasks,cn=config
有效值	0 到 65534
默认值	无
语法	整数
示例	replica-id: 55

2.26. CN=TASK_NAME,CN=ABORT CLEANALLRUV,CN=TASKS,CN=CONFIG

cleanall 任务可能需要几分钟时间来在复制拓扑中的所有服务器之间传播，即使任务首先处理所有更新也是如此。对于性能或其他维护注意事项，可以终止干净的 RUV 任务，并且该终止也会在复制拓扑中的所有服务器之间传播。

termination 任务是 cn=abort cleanallruv 条目的实例。

任务完成后，任务条目会从目录中删除。

cn=abort cleanallruv 条目是所有清理 RUV 操作的容器条目。cn=abort cleanallruv 条目本身没有与任何单个任务相关的属性，但此条目下的每个任务条目（如 cn=task_ID,cn=abort cleanallruv,cn=tasks,cn=config ）都使用其属性来定义单独的更新任务。

每个清理 RUV 任务必须指定 当前要删除的 副本 RUV 条目的副本 ID 号、复制数据库的基于 DN，以及终止任务是否应该在拓扑中的所有服务器上完成，还是在本地的服务器上完成。

```
dn: cn=abort 55,cn=abort cleanallruv,cn=tasks,cn=config
objectclass: extensibleObject
replica-base-dn: dc=example,dc=com
replica-id: 55
replica-certify-all: yes
cn: abort 55
```

2.26.1. replica-base-dn

这提供了与复制数据库关联的目录服务器基本 DN。这是复制后缀的基本 DN。

参数	描述
条目 DN	cn=*task_name*,cn=abort cleanallruv,cn=tasks,cn=config
有效值	目录后缀 DN
默认值	无
语法	DirectoryString
示例	replica-base-dn: dc=example,dc=com

2.26.2. replica-certify-all

这个设置会在本地完成任务前，在复制拓扑中的所有服务器上成功完成任务(yes)，或者任务是否应该在本地完成后立即完成(无)。

参数	描述
条目 DN	cn=*task_name*,cn=abort cleanallruv,cn=tasks,cn=config
有效值	No | yes
默认值	无
语法	DirectoryString
示例	replica-certify-all: yes

2.26.3. replica-id

这提供了从复制拓扑中删除副本配置条目的 nsDS5ReplicaId 属性中的副本 ID（在 nsDS5ReplicaId 属性中定义）。

参数	描述
条目 DN	cn=*task_name*,cn=abort cleanallruv,cn=tasks,cn=config
有效值	0 到 65534

参数	描述
默认值	无
语法	整数
示例	replica-id: 55

2.27. CN=TASK_NAME,CN=AUTOMEMBER REBUILD MEMBERSHIP,CN=TASKS,CN=CONFIG

Auto Member 插件仅在向目录中添加新条目时运行。该插件会忽略编辑的现有条目或条目，以匹配自动成员规则。

cn=automember rebuild membership 任务针对 现有条目 运行当前的自动成员规则，以更新或重建组成员资格。所有配置的自动成员规则都针对指定的条目运行（但并非所有规则都可能应用到给定条目）。

2.27.1. basedn

这提供了用于搜索用户条目的目录服务器基本 DN。然后，根据自动成员规则更新指定 DN 中的条目。

参数	描述
条目 DN	cn=*task_name*,cn=automember rebuild membership,cn=tasks,cn=config
有效值	目录后缀 DN
默认值	无
语法	DirectoryString
示例	basedn: dc=example,dc=com

2.27.2. filter

此属性提供了一个 LDAP 过滤器，用于根据配置的自动成员规则来识别要更新哪些用户条目。

参数	描述
条目 DN	cn=*task_name*,cn=automember rebuild membership,cn=tasks,cn=config
有效值	任何 LDAP 过滤器
默认值	无
语法	DirectoryString
示例	filter: (uid.4-1.)

2.27.3. scope

此属性提供在搜索给定基本 DN 时使用的 LDAP 搜索范围。

参数	描述
条目 DN	cn=*task_name*,cn=automember rebuild membership,cn=tasks,cn=config
有效值	sub | 基础 | 一个
默认值	无
语法	DirectoryString
示例	scope: sub

2.28. CN=TASK_NAME,CN=AUTOMEMBER EXPORT UPDATES,CN=TASKS,CN=CONFIG

此任务针对目录中 现有条目 运行，并根据规则导出将哪些用户添加到哪些组中的结果。这可用于针对现有用户测试现有规则，以查看您的实际部署是如何执行的。

不执行与自动成员资格 相关的更改。建议的更改将写入指定的 LDIF 文件。

2.28.1. basedn

这提供了用于搜索用户条目的目录服务器基本 DN。针对标识的条目运行自动成员规则的测试运行。

参数	描述
条目 DN	cn=*task_name*,cn=automember export updates,cn=tasks,cn=config
有效值	目录后缀 DN
默认值	无
语法	DirectoryString
示例	basedn: dc=example,dc=com

2.28.2. filter

此属性提供 LDAP 过滤器，用于识别要测试的自动成员规则的用户条目。

参数	描述
条目 DN	cn=*task_name*,cn=automember export updates,cn=tasks,cn=config
有效值	任何 LDAP 过滤器
默认值	无
语法	DirectoryString
示例	filter: (uid.4-1.)

2.28.3. ldif

此属性设置 LDIF 文件的完整路径和文件名，该文件将从自动成员规则的 test-run 中写入所提议的更改。此文件必须是启动任务的系统的本地文件。

参数	描述
条目 DN	cn=*task_name*,cn=automember export updates,cn=tasks,cn=config
有效值	本地路径和文件名

参数	描述
默认值	无
语法	DirectoryString
示例	ldif: /tmp/automember-results.ldif

2.28.4. scope

此属性提供在搜索给定基本 DN 时使用的 LDAP 搜索范围。

参数	描述
条目 DN	cn=*task_name*,cn=automember export updates,cn=tasks,cn=config
有效值	sub | 基础 | 一个
默认值	无
语法	DirectoryString
示例	scope: sub

2.29. CN=TASK_NAME,CN=AUTOMEMBER MAP UPDATES,CN=TASKS,CN=CONFIG

此任务针对 LDIF 文件中的条目（新条目或潜在的测试条目）运行，然后将所提议的更改写入 LDIF 文件。在将新规则应用到（真实）新的或现有用户条目之前，这对测试新规则非常有用。

不执行与自动成员资格 相关的更改。建议的更改将写入指定的 LDIF 文件。

2.29.1. ldif_in

此属性设置 LDIF 文件的完整路径和文件名，从中导入条目以使用配置的自动成员规则进行测试。这些条目没有导入到目录中，且不会执行更改。该条目由 test-run 加载和使用。

此文件必须是启动任务的系统的本地文件。

参数	描述
条目 DN	cn=*task_name*,cn=automember map updates,cn=tasks,cn=config
有效值	本地路径和文件名
默认值	无
语法	DirectoryString
示例	ldif_in: /tmp/automember-test-users.ldif

2.29.2. ldif_out

此属性设置 LDIF 文件的完整路径和文件名，该文件将从自动成员规则的 test-run 中写入所提议的更改。此文件必须是启动任务的系统的本地文件。

参数	描述
条目 DN	cn=*task_name*,cn=automember map updates,cn=tasks,cn=config
有效值	本地路径和文件名
默认值	无
语法	DirectoryString
示例	ldif_out: /tmp/automember-results.ldif

2.30. CN=TASK_NAME,CN=DES2AES,CN=TASKS,CN=CONFIG

此任务搜索指定用户数据库中的所有反向密码条目，这些条目使用过时的 DES 密码进行编码，并将其转换为更安全的 AES 密码。

在以前的版本中，此任务会在 Directory Server 启动过程中自动在所有后缀上执行。但是，由于搜索 DES 密码通常不会索引，所以在包含大量条目的后缀上执行非常长的时间，从而导致目录服务器超时并无法启动。因此，搜索现在只在 cn=config 上执行，但若要在任何其他数据库中转换密码，您必须手动运行此任务。

2.30.1. suffix

这个多值属性指定一个后缀来检查 DES 密码并将其转换为 AES。如果省略此属性，则将检查所有后端/后缀。

参数	描述
条目 DN	cn=*task_name*,cn=des2aes,cn=tasks,cn=config
有效值	目录后缀 DN
默认值	无
语法	DirectoryString
示例	suffix: dc=example,dc=com

2.31. ROOT DSE 配置参数

2.31.1. nsslapd-return-default-opattr

目录服务器不会在 Root DSE 搜索中显示操作属性。例如，如果您使用 -s base -b "" 参数运行 ldapsearch 工具，则只会显示用户属性。对于在 Root DSE 搜索输出中预期操作属性的客户端，您可以启用此行为来提供向后兼容性：

1. *停止 Directory 服务器实例。*
2. *编辑 /etc/dirsrv/slapd-instance_name/dse.ldif 文件，并将以下参数添加到 dn: 部分：*

```
nsslapd-return-default-opattr: supportedsaslmechanisms
nsslapd-return-default-opattr: nsBackendSuffix
nsslapd-return-default-opattr: subschemasubentry
nsslapd-return-default-opattr: supportedldapversion
nsslapd-return-default-opattr: supportedcontrol
nsslapd-return-default-opattr: ref
nsslapd-return-default-opattr: vendorname
nsslapd-return-default-opattr: vendorVersion
nsslapd-return-default-opattr: supportedextension
nsslapd-return-default-opattr: namingcontexts
```

3. *启动 Directory 服务器实例。*

参数	描述
条目 DN	root DSE
有效值	supportedsaslmechanisms | nsBackendSuffix | subschemasubentry | supportedldapversion | supportedcontrol | ref | vendorname | vendorVersion
默认值	
语法	DirectoryString
示例	nsslapd-return-default-opattr: supportedsaslmechanisms

第 3 章 配置对象类

许多配置条目只是使用 extensibleObject 对象类，但有些需要其他对象类。这些配置对象类列在此处。

3.1. CHANGELOGENTRY

此对象类用于存储对 Directory Server 条目所做的更改的条目。

要将目录服务器配置为维护与目录服务器 4.1x 中实施的 changelog 兼容，请启用 Retro Changelog 插件。changelog 中的每个条目都有 changeLogEntry 对象类。

这个对象类在 Changelog Internet Draft 中定义。

优越的类

top

OID

2.16.840.1.113730.3.2.1

表 3.1. 必要属性

objectClass	定义条目的对象类。
changeNumber	包含为更改日志随机分配的数字。
changeTime	更改发生的时间。
changeType	在条目上执行的更改类型。
targetDn	在供应商服务器上添加、修改或删除的条目的区分名称。

表 3.2. 允许的属性

更改	对目录服务器所做的更改。

deleteOldRdn	定义条目的旧 Relative Distinguished Name (RDN)的标志应保留为条目的可分辨属性或应该被删除。
newRdn	作为 modRDN 或 modDN 操作目标的条目的新 RDN。
newSuperior	在处理 modDN 操作时，它成为现有条目的即时越好条目的名称。

3.2. DIRECTORYSERVERFEATURE

此对象类专门用于识别目录服务功能的条目。此对象类由 Directory Server 定义。

优越的类

top

OID

2.16.840.1.113730.3.2.40

表 3.3. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。

表 3.4. 允许的属性

属性	定义
cn	指定条目的通用名称。
multiLineDescription	提供条目的文本描述。
OID	指定功能的 OID。

3.3. NSBACKENDINSTANCE

此对象类用于目录服务器后端或数据库实例条目。此对象类在 Directory Server 中定义。

优越的类

top

OID

2.16.840.1.113730.3.2.109

表 3.5. 必要属性

属性	定义
objectClass	定义条目的对象类。
cn	提供条目的通用名称。

3.4. NSDS5REPLICA

此对象类用于定义数据库复制中的副本的条目。其中许多属性都在后端中设置，且无法修改。

有关此对象类的属性的信息，其列出了 目录服务器配置、命令和文件参考 的第 2 章的核心配置属性。

此对象类在 Directory Server 中定义。

优越的类

top

OID

2.16.840.1.113730.3.2.108

表 3.6. 必要属性

objectClass	定义条目的对象类。
nsDS5ReplicaId	指定复制环境中供应商的唯一 ID。
nsDS5ReplicaRoot	指定复制区域根目录的后缀 DN。

表 3.7. 允许的属性

cn	指定副本的名称。
nsDS5Flags	指定之前在标志中设置的信息。
nsDS5ReplicaAutoReferral	设置服务器是否遵循为 Directory Server 数据库配置的引用。
nsDS5ReplicaBindDN	指定供应商服务器绑定到消费者时使用的 DN。
nsDS5ReplicaChangeCount	提供更改日志中的条目总数以及是否复制它们。
nsDS5ReplicaLegacyConsumer	指定副本是否为旧的消费者。
nsDS5ReplicaName	指定内部操作的副本的唯一 ID。
nsDS5ReplicaPurgeDelay	指定更改日志清除前的时间（以秒为单位）。
nsDS5ReplicaReferral	指定用户定义的引用的 URL。
nsDS5ReplicaReleaseTimeout	指定供应商将发布副本的超时，无论它是否完成发送更新。
nsDS5ReplicaTombstonePurgeInterval	指定清除操作周期之间的时间间隔（以秒为单位）。
nsDS5ReplicaType	定义副本的类型，如只读消费者。
nsDS5Task	启动复制任务，如将数据库内容转储到 LDIF；这由目录服务器供应商在内部使用。
nsState	存储有关时钟的信息，以便生成正确更改序列号。

3.5. NSDS5REPLICATIONAGREEMENT

*带有 **nsDS5ReplicationAgreement** 对象类的条目存储复制协议中设置的信息。有关此对象类的属性的信息，请参见 目录服务器配置、命令和文件参考 中的第 2 章。*

*此对象类在 **Directory Server** 中定义。*

优越的类

top

OID

2.16.840.1.113730.3.2.103

表 3.8. 必要属性

objectClass	定义条目的对象类。
cn	用于命名复制协议。

表 3.9. 允许的属性

description	包含复制协议的自由文本描述。
nsDS5BeginReplicaRefresh	手动初始化副本。
nsds5debugreplicatimeout	提供一个在使用调试日志记录运行时使用的替代超时时间。
nsDS5ReplicaBindDN	指定供应商服务器绑定到消费者时使用的 DN。
nsDS5ReplicaBindMethod	指定用于绑定的方法(SSL 或简单身份验证)。
nsDS5ReplicaBusyWaitTime	指定供应商在进行另一个尝试获取访问前，在消费者发送忙碌响应后等待的时间（以秒为单位）。
nsDS5ReplicaChangesSentSinceStartup	从服务器启动以来发送到此副本的更改数量。
nsDS5ReplicaCredentials	指定绑定 DN 的密码。
nsDS5ReplicaHost	指定消费者副本的主机名。
nsDS5ReplicaLastInitEnd	消费者副本初始化结束时的状态。
nsDS5ReplicaLastInitStart	消费者副本初始化启动时的状态。
nsDS5ReplicaLastInitStatus	消费者初始化的状态。
nsDS5ReplicaLastUpdateEnd	当最新复制调度更新结束时显示。
nsDS5ReplicaLastUpdateStart	最近的复制调度更新启动时状态。
nsDS5ReplicaLastUpdateStatus	提供最新复制调度更新的状态。
nsDS5ReplicaPort	指定远程副本的端口号。
nsDS5ReplicaRoot	指定复制区域根目录的后缀 DN。

nsDS5ReplicaSessionPauseTime	指定供应商在更新会话之间等待的时间（以秒为单位）。
nsDS5ReplicatedAttributeList	指定不会复制到消费者服务器的任何属性。
nsDS5ReplicaTimeout	指定出站 LDAP 操作的秒数，在超时和失败前等待远程副本的响应。
nsDS5ReplicaTransportInfo	指定用于将数据传输到副本或从副本传输数据的传输类型。
nsDS5ReplicaUpdateInProgress	说明复制调度更新是否正在进行中。
nsDS5ReplicaUpdateSchedule	指定复制调度。
nsDS50ruv	使用复制更新向量管理副本的内部状态。
nsruvReplicaLastModified	包含最近一个副本中的条目被修改的时间，并且更改日志已更新。
nsds5ReplicaStripAttrs	使用 fractional replication 时，对 exclude 属性的更新仍然会触发复制事件，但该事件为空。此属性设置从复制更新中剥离的属性。这可防止对 **internalModifyTimestamp** 等属性的更改触发空复制更新。

3.6. NSDSWINDOWSREPLICATIONAGREEMENT

存储与同步协议相关的同步属性。有关此对象类的属性的信息，请参见 {PRODUCT} 配置、命令和文件参考中的 第 2 章。

此对象类在 Directory Server 中定义。

优越的类

top

OID

2.16.840.1.113730.3.2.503

表 3.10. 必要属性

objectClass	定义条目的对象类。
cn	提供同步协议的名称。

表 3.11. 允许的属性

description	包含同步协议的文本描述。
nsDS5BeginReplicaRefresh	启动手动同步。
nsds5debugreplicatimeout	给出一个替代的超时时间，以便在同步使用 debug 日志记录运行时使用。
nsDS5ReplicaBindDN	指定在 Directory 服务器绑定到 Windows 服务器时要使用的 DN。
nsDS5ReplicaBindMethod	指定用于绑定的方法(SSL 或简单身份验证)。
nsDS5ReplicaBusyWaitTime	指定目录服务器在进行另一个尝试获取访问前，在 Windows 服务器发送回忙响应后应等待的时间（以秒为单位）。
nsDS5ReplicaChangesSentSinceStartup	显示目录服务器启动后发送的更改数量。
nsDS5ReplicaCredentials	指定绑定 DN 的凭证。
nsDS5ReplicaHost	指定要同步的 Windows 服务器的 Windows 域控制器的主机名。
nsDS5ReplicaLastInitEnd	当 Windows 服务器最后一次更新（重新同步）时的状态。
nsDS5ReplicaLastInitStart	当 Windows 服务器最近一次更新（重新同步）时，状态。
nsDS5ReplicaLastInitStatus	Windows 服务器更新总数（重新同步）的状态。
nsDS5ReplicaLastUpdateEnd	最近更新结束时显示。
nsDS5ReplicaLastUpdateStart	最近一次更新启动时的状态。
nsDS5ReplicaLastUpdateStatus	提供最新更新的状态。
nsDS5ReplicaPort	指定 Windows 服务器的端口号。
nsDS5ReplicaRoot	指定目录服务器的根后缀 DN。

nsDS5ReplicaSessionPauseTime	指定 Directory 服务器在更新会话之间应等待的时间（以秒为单位）。
nsDS5ReplicaTimeout	指定出站 LDAP 操作将在超时和失败前等待 Windows 服务器响应的秒数。
nsDS5ReplicaTransportInfo	指定用于将数据传输到 Windows 服务器的传输类型。
nsDS5ReplicaUpdateInProgress	说明更新是否正在进行中。
nsDS5ReplicaUpdateSchedule	指定同步调度。
nsDS50ruv	使用复制更新向量(RUV)管理目录服务器同步对等的内部状态。
nsds7DirectoryReplicaSubtree	指定同步的目录服务器后缀（根或子）。
nsds7DirsyncCookie	包含由同步服务设置的 Cookie，充当 RUV。
nsds7NewWinGroupSyncEnabled	指定是否在 Directory 服务器上自动创建新的 Windows 组帐户。
nsds7NewWinUserSyncEnabled	指定是否在 Directory 服务器上自动创建新的 Windows 用户帐户。
nsds7WindowsDomain	标识正在同步的 Windows 域；类似于复制协议中的 **nsDS5ReplicaHost**。
nsds7WindowsReplicaSubtree	指定同步的 Windows 服务器后缀（根或子）。
nsruvReplicaLastModified	包含 Directory Server sync peer 中的条目被修改的最新时间，并更新了 changelog。
winSyncInterval	设置目录服务器轮询 Windows 服务器要写入的频率，以秒为单位。如果没有设置，则默认为 **300** 秒，即 300 秒或 5 分钟。
winSyncMoveAction	设置 sync 插件如何处理同步子树外 Active Directory 中发现的对应条目。同步过程可以忽略这些条目 (none、默认条目)，或者可以假定条目被有意从同步中移除，然后它可以删除对应的目录服务器条目（删除）或删除同步属性，并且不再同步条目(unsync)。

3.7. NSENCRYPTIONCONFIG

***nsEncryptionConfig** 对象类存储允许的加密选项的配置信息，如协议和密码套件。这在管理服务中定义。*

优越的类

top

OID

nsEncryptionConfig-oid

表 3.12. 必要属性

属性	定义
objectClass	定义条目的对象类。
cn (commonName)	提供设备的通用名称。

表 3.13. 允许的属性

属性	定义
nsSSL3SessionTimeout	为 SSLv3 密码会话设置超时周期。
nsSSLClientAuth	设置服务器如何处理客户端身份验证。有三个可能的值： allow、disallow 或 require。
nsSSLSessionTimeout	为密码会话设置超时周期。
nsSSLSupportedCiphers	包含可用于到服务器的安全连接的所有密码的列表。
nsTLS1	设置是否为服务器启用 TLS 版本 1。

3.8. NSENCRYPTIONMODULE

nsEncryptionModule 对象类存储加密模块信息。这在管理服务中定义。

优越的类

top

OID

nsEncryptionModule-oid

表 3.14. 必要属性

属性	定义
objectClass	定义条目的对象类。
cn (commonName)	提供设备的通用名称。

表 3.15. 允许的属性

属性	定义
nsSSLActivation	设置是否启用密码系列。
nsSSLPersonalitySSL	包含服务器用于 SSL 的证书名称。
nsSSLToken	标识服务器使用的安全令牌。

3.9. NSMAPPINGTREE

映射树将后缀映射到后端。每个映射树条目都使用 nsMappingTree 对象类。此对象类在 Directory Server 中定义。

优越的类

top

OID

2.16.840.1.113730.3.2.110

表 3.16. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
cn	提供条目的通用名称。

3.10. NSSASLMAPPING

此对象类用于包含将 SASL 属性映射到目录服务器属性的身份映射配置的条目。

此对象类在 Directory Server 中定义。

优越的类

top

OID

2.16.840.1.113730.3.2.317

表 3.17. 必要属性

objectClass	定义条目的对象类。
cn	指定 SASL 映射条目的名称。
nsSaslMapBaseDNTemplate	包含搜索基础 DN 模板。
nsSaslMapFilterTemplate	包含搜索过滤器模板。
nsSaslMapRegexString	包含一个匹配 SASL 身份字符串的正则表达式。

3.11. NSSLAPDCONFIG

nsslapdConfig 对象类为 Directory Server 实例定义配置对象 cn=config。

此对象类在 Directory Server 中定义。

优越的类

top

OID

2.16.840.1.113730.3.2.39

表 3.18. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。

表 3.19. 允许的属性

属性	定义
cn	提供条目的通用名称。

3.12. PASSWORDPOLICY

local 和 global 密码策略都使用 passwordPolicy 对象类。此对象类在 Directory Server 中定义。

优越的类

top

OID

2.16.840.1.113730.3.2.13

表 3.20. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。

表 3.21. 允许的属性

属性	定义
passwordMaxAge	设置用户密码过期的秒数。
passwordExp	标识用户的密码是否在 'passwordMaxAge' 属性给出的间隔后过期。
passwordMinLength	设置密码中必须要使用的最少字符数。
passwordInHistory	设置目录中存储在历史记录中的密码数量。
passwordChange	确定是否允许用户更改自己的密码。

属性	定义
passwordWarning	设置警告消息发送到密码即将过期的用户前的秒数。
passwordLockout	确定在给定数量的绑定尝试失败后是否锁定了目录。
passwordMaxFailure	设置用户锁定目录后失败的绑定尝试次数。
passwordUnlock	标识用户是否已锁定，直到管理员重置密码，或者用户在给定的锁定持续时间后再次登录。默认为允许用户在锁定期后重新登录。
passwordLockoutDuration	设置用户将被锁定在目录中的时间（以秒为单位）。
passwordCheckSyntax	确定服务器是否在保存密码前检查密码语法。
passwordMustChange	标识在首次登录到目录时或 Directory Manager 重置密码后是否更改密码。
passwordStorageScheme	设置用于存储目录服务器密码的加密类型。
passwordMinAge	设置在用户更改密码前必须经过的秒数。
passwordResetFailureCount	设置时间（以秒为单位），之后将重置密码失败计数器。每次从用户帐户发送无效的密码时，密码失败计数器都会递增。
passwordGraceLimit	设置在用户的密码过期时允许的宽限期数量。
passwordMinDigits	设置必须在密码中使用的最少数字字符(0 到 9)。
passwordMinAlphas	设置密码中必须要使用的最少字母字符数。
passwordMinUppers	设置大写字符(A 到 Z)的最小大写字符数，该字符必须在密码中使用。
passwordMinLowers	设置大小最低的字母字符数，a 到 z，该字符必须在密码中使用。
passwordMinSpecials	设置最小特殊 ASCII 字符数，如 **!@#$.**，该字符必须在密码中使用。
passwordMin8Bit	设置密码中使用的最少 8 位 chracters 数量。
passwordMaxRepeats	设置可连续使用相同字符的次数上限。
passwordMinCategories	设置密码中必须使用的最小类别数。

属性	定义
passwordMinTokenLength	设置检查普通词语的长度。
passwordTPRDelayValidFrom	当临时密码有效时设置延迟。
passwordTPRDelayExpireAt	设置临时密码有效的秒数。
passwordTPRMaxUse	设置可以使用临时密码的最大尝试次数。

第 4 章 CN=MONITOR

用于监控服务器的信息存储在 cn=monitor 下。此条目及其子项是只读的；客户端无法直接修改它们。服务器自动更新此信息。本节论述了 cn=monitor 属性。用户可以更改的唯一属性来设置访问控制。

如果 cn=config 中的 nsslapd-counters 属性设为 on （默认设置），则目录服务器实例保留的所有计数器都会使用 64 位整数递增，即使 32 位机器或 32 位目录服务器版本。对于 cn=monitor 条目，64 位整数用于 opsinitiated,opscompleted,entriessent, 和 bytessent 计数器。

注意

nsslapd-counters 属性为这些特定的数据库和服务器计数器启用 64 位支持。使用 64 位整数的计数器不可配置；所有允许的计数器都启用了 64 位整数，或为所有允许的计数器禁用。

4.1. BACKENDMONITORDN

此属性显示每个目录服务器数据库后端的 DN。有关监控数据库的详情，请查看以下部分：

- 第 6.4.10 节 “cn=attribute_name,cn=encrypted attributes,cn=database_name,cn=ldbm database,cn=plugins,cn=config 下的数据库属性”
- 第 6.4.5 节 “cn=database,cn=monitor,cn=ldbm database,cn=plugins,cn=config 下的数据库属性”
- 第 6.5.4 节 “cn=monitoring,cn=database_link_name,cn=chaining database,cn=plugins,cn=config 下的数据库链接属性”

4.2. BYTESSENT

此属性显示 Directory 服务器发送的字节数。

4.3. 连接

此属性列出打开的连接和相关状态，以及与性能相关的信息和值。它们以以下格式提供：

```
connection: pass:quotes[A:YYYYMMDDhhmmssZ:B:C:D:E:F:G:H:I:IP_address]
```

例如：

```
connection: pass:quotes[69:20200604081953Z:6086:6086:-
:cn=proxy,ou=special_users,dc=example,dc=test:0:11:27:7448846:ip=192.0.2.1]
```

- A 是连接号，这是与此连接关联的连接表中的插槽数量。这是打开此连接时在访问日志消息中作为 slot=A 记录的编号，通常与连接关联的文件描述符对应。属性 dTableSize 显示连接表的总大小。
- yyyymmddHHMMSSZ 是打开连接的日期和时间，格式为 GeneralizedTime。这个值提供了与 Greenwich Mean Time 相关的时间。
- b 是此连接上收到的操作数量。
- c 是已完成的操作的数量。
- 如果服务器 位于从网络读取 BER 的过程，则 d 为 r，否则为空。这个值通常为空（如示例中）。
- 这是 绑定 DN。这可以为空，或者对于匿名连接具有 NULLDN 的值。
- f 是连接最大线程状态： 1 处于最大线程，0 代表不是。
- g 是此线程达到最大线程值的次数。
- H 是受最大线程数阻止的操作数量。
- 我是 日志中报告的连接 ID 为 conn=connection_ID。
- ip_address 是 LDAP 客户端的 IP 地址。

注意

理想情况下，用于启动和完成操作的 b 和 C 应该相等。

4.4. CURRENTCONNECTIONS

此属性显示当前打开和活跃的目录服务器连接的数量

4.5. CURRENTTIME

此属性显示当前的时间，在 Greenwich Mean Time 中给出（通过常规的Time 语法 Z 表示法表示；例如，202 20202131102Z）。

4.6. DTABLESIZE

dTableSize 属性显示目录服务器连接表的大小。每个连接都与此表中的一个插槽关联，通常对应于此连接使用的文件描述符。如需更多信息，请参阅 nsslapd-maxdescriptors 和 nsslapd-reservedescriptors。

4.7. ENTRIESSENT

此属性显示 Directory 服务器发送的条目数。

4.8. NBACKENDS

此属性显示目录服务器数据库后端的数量。

4.9. OPSINITIATED

此属性显示已完成的目录服务器操作数量。

4.10. READWAITERS

此属性显示某些请求待处理且目前由 Directory Server 中的线程服务的连接数量。

4.11. STARTTIME

此属性显示 Greenwich Mean Time 中给定的目录服务器启动时间，使用常规的Time 语法 Z 表示法表示。例如，202 20202131102Z。

4.12. THREADS

此属性显示 Directory 服务器使用的线程数量。这应该与 cn=config 中的 nsslapd-threadnumber 对应。

4.13. TOTALCONNECTIONS

此属性显示目录服务器连接的总数。此数字包括自服务器上次启动后打开和关闭的连接，除了 currentConnections 外。

4.14. VERSION

此属性显示 Directory Server vendor、 version 和 build number。例如： 389-Directory/2.0.14 B2022.082.0000。

第 5 章 ROOT DSE 属性

本节中的属性用于定义服务器实例的根目录(DSE)。DSE 中定义的信息与服务器实例的实际配置相关，如该服务器软件版本中支持的控制、机制或功能。它还包含特定于实例的信息，如其构建号和安装日期。

DSE 是一个特殊条目，位于正常的 DIT 之外，可以通过使用 null 搜索基础进行搜索来返回。例如：

```
# ldapsearch -D "cn=Directory Manager" -W -p 389 -h server.example.com -x -s base -b ""
"objectclass=*"
```

5.1. DATAVERSION

此属性包含一个时间戳，其中显示了目录中任何数据的最近编辑时间。

```
dataversion: 020090923175302020090923175302
```

OID	
语法	GeneralizedTime
multi- 或 Single-Valued	单值
定义在	目录服务器

5.2. DEFAULTNAMINGCONTEXT

对应于命名上下文，除了所有配置的命名上下文中，客户端应默认使用这些命名上下文。

OID	
语法	DN
multi- 或 Single-Valued	单值
定义在	目录服务器

5.3. LASTUSN

每当写入操作 - add, modify, delete, 和 modrdn - 对该条目执行时，都会为每个条目分配一个序列号。USN 在条目的 entryUSN 操作属性中分配。

USN 插件有两种模式：local 和 global。

在本地模式中，为服务器实例维护的每个数据库都有自己的 USN 插件实例，每个后端数据库都有一个单独的 USN 计数器。为数据库中的任何条目分配的最新 USN 显示在 lastusn 属性中。当 USN 插件设置为 local 模式时，lastUSN 属性会显示分配了 USN 和 USN 的数据库：

```
lastusn;database_name:USN
```

例如：

```
lastusn;example1: 213
lastusn;example2: 207
```

在全局模式中，当数据库使用共享 USN 计数器时，lastUSN 值会显示由任何数据库分配的最新 USN：

```
lastusn: 420
```

5.4. NAMINGCONTEXTS

对应于服务器控制或影子的命名上下文。当目录服务器不控制任何信息（比如当它是公共 X.500 目录的 LDAP 网关）时，此属性不存在。当目录服务器认为它包含整个目录时，属性具有单个值，而该值是空字符串（代表 root 的 null DN）。此属性允许客户端联系服务器以选择合适的基础对象进行搜索。

OID	1.3.6.1.4.1.1466.101.120.5
语法	DN
multi- 或 Single-Valued	多值
定义在	RFC 2252

5.5. NETSCAPEMDSUFFIX

此属性包含服务器中维护机器数据的目录树的 top 后缀的 DN。DN 本身指向 LDAP URL。例如：

> *cn=ldap://dc=pass:quotes[server_name],dc=example,dc=com:389*

OID	2.16.840.1.113730.3.1.212
语法	DN
multi- 或 Single-Valued	单值
定义在	目录服务器

5.6. SUPPORTEDCONTROL

此属性的值是用于标识服务器支持的控制的对象标识符(OID)。当服务器不支持控制时，此属性不存在。

OID	1.3.6.1.4.1.1466.101.120.13
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2252

5.7. SUPPORTEDEXTENSION

此属性的值是用于标识服务器支持的扩展操作的对象标识符(OID)。当服务器不支持扩展操作时，缺少此属性。

OID	1.3.6.1.4.1.1466.101.120.7
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2252

5.8. SUPPORTEDFEATURES

此属性包含当前 {PRODUCT} 支持的功能。

OID	1.3.6.1.4.1.4203.1.3.5
语法	OID
multi- 或 Single-Valued	多值
定义在	RFC 3674

5.9. SUPPORTEDLDAPVERSION

此属性标识服务器实施的 LDAP 协议的版本。

OID	1.3.6.1.4.1.1466.101.120.15
语法	整数
multi- 或 Single-Valued	多值
定义在	RFC 2252

5.10. SUPPORTEDSASLMECHANISMS

此属性标识服务器支持的 SASL 机制的名称。当服务器不支持 SASL 属性时，这个属性不存在。

OID	1.3.6.1.4.1.1466.101.120.14
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2252

5.11. VENDORNAME

此属性包含服务器厂商的名称。

OID	1.3.6.1.1.4
语法	DirectoryString

multi- 或 Single-Valued	单值
定义在	RFC 3045

5.12. VENDORVERSION

此属性显示服务器的厂商版本号。

OID	1.3.6.1.1.5
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	RFC 3045

config-schema-reference-title

第 6 章 插件实现的服务器功能参考

本章包含插件的参考信息。

Directory 服务器插件功能的每个部分的配置在子树 cn=plugins,cn=config 下都有自己的独立条目和属性集。

```
dn: cn=Telephone Syntax,cn=plugins,cn=config
objectclass: top
objectclass: nsSlapdPlugin
objectclass: extensibleObject
cn: Telephone Syntax
nsslapd-pluginPath: libsyntax-plugin
nsslapd-pluginInitfunc: tel_init
nsslapd-pluginType: syntax
nsslapd-pluginEnabled: on
```

其中一些属性适用于所有插件，而其他插件则可能特定于特定的插件。您可以通过在 cn=config 子树上执行 ldapsearch 来检查给定插件使用哪些属性。

所有插件都是从 extensibleObject 对象类继承的 nsSlapdPlugin 对象类的实例。当条目中存在两个对象类（除顶级对象类外）时，服务器会考虑插件配置属性，如下例所示：

```
dn:cn=ACL Plugin,cn=plugins,cn=config
objectclass:top
objectclass:nsSlapdPlugin
objectclass:extensibleObject
```

6.1. 所有插件通用属性列表

此列表提供了简短的属性描述、条目 DN、有效范围、默认值、语法和每个属性的示例。

每个目录服务器插件都属于 nsslapdPlugin 对象类。

此对象类在 Directory Server 中定义。

优越的类

top

OID

2.16.840.1.113730.3.2.41

表 6.1. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
cn	提供条目的通用名称。
nsslapd-pluginPath	标识插件库名称（不带库后缀）。
nsslapd-pluginInitfunc	标识插件的初始化功能。
nsslapd-pluginType	标识插件的类型。
nsslapd-pluginId	标识插件 ID。
nsslapd-pluginVersion	标识插件的版本。
nsslapd-pluginVendor	标识插件的供应商。
nsslapd-pluginDescription	标识插件的描述。
nsslapd-pluginEnabled	标识是否启用插件。
nsslapd-pluginPrecedence	按照执行顺序设置插件的优先级。

6.1.1. nsslapd-logAccess

此属性允许您将插件运行的搜索操作记录到 cn=config 中的 nsslapd-accesslog 参数中设置的文件。

插件参数	描述
条目 DN	cn=plug-in name,cn=plugins,cn=config
有效值	on | off
默认值	off

插件参数	描述
语法	DirectoryString
示例	nsslapd-logAccess: Off

6.1.2. nsslapd-logAudit

此属性允许您记录和审核数据库修改，源自插件。

如果在 cn=config 中启用了 nsslapd-auditlog-logging-enabled 参数，则成功修改事件会记录在审计日志中。要通过插件记录失败的修改数据库操作，请在 cn=config 中启用 nsslapd-auditfaillog-logging-enabled 属性。

插件参数	描述
条目 DN	cn=plug-in name,cn=plugins,cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-logAudit: Off

6.1.3. nsslapd-pluginDescription

此属性提供插件的描述。

插件参数	描述
条目 DN	cn=plug-in name,cn=plugins,cn=config
有效值	
默认值	无
语法	DirectoryString
示例	nsslapd-pluginDescription: acl access check 插件

6.1.4. nsslapd-pluginEnabled

此属性指定插件是否已启用。可以使用协议更改此属性，但仅在下一次服务器重启时生效。

插件参数	描述
条目 DN	cn=plug-in name,cn=plugins,cn=config
有效值	on | off
默认值	on
语法	DirectoryString
示例	nsslapd-pluginEnabled: on

6.1.5. nsslapd-pluginId

此属性指定插件 ID。

插件参数	描述
条目 DN	cn=plug-in name,cn=plugins,cn=config
有效值	任何有效的插件 ID
默认值	无
语法	DirectoryString
示例	nsslapd-pluginId: chaining database

6.1.6. nsslapd-pluginInitfunc

此属性指定要启动插件功能。

插件参数	描述
条目 DN	cn=plug-in name,cn=plugins,cn=config
有效值	任何有效的插件功能

插件参数	描述
默认值	无
语法	DirectoryString
示例	nsslapd-pluginInitfunc: NS7bitAttr_Init

6.1.7. nsslapd-pluginPath

此属性指定插件的完整路径。

插件参数	描述
条目 DN	cn=plug-in name,cn=plugins,cn=config
有效值	任何有效的路径
默认值	无
语法	DirectoryString
示例	nsslapd-pluginPath: uid-plugin

6.1.8. nsslapd-pluginPrecedence

此属性设置插件执行顺序的优先级或优先级。优先级定义插件的执行顺序，允许更复杂的环境或交互，因为它可以在执行前等待完成的操作。对于 pre-operation 和 post-operation 插件，这更为重要。

值 1 的插件具有最高的优先级，首先运行；值为 99 的插件具有最低优先级。默认值为 50.

插件参数	描述
条目 DN	cn=plug-in name,cn=plugins,cn=config
有效值	1 到 99
默认值	50
语法	整数

插件参数	描述
示例	nsslapd-pluginPrecedence: 3

6.1.9. nsslapd-pluginType

此属性指定插件类型。如需更多信息，请参阅 第 6.2.4 节 “nsslapd-plugin-depends-on-type”。

插件参数	描述
条目 DN	cn=plug-in name,cn=plugins,cn=config
有效值	任何有效的插件类型
默认值	无
语法	DirectoryString
示例	nsslapd-pluginType: preoperation

6.1.10. nsslapd-pluginVendor

此属性指定插件的供应商。

插件参数	描述
条目 DN	cn=plug-in name,cn=plugins,cn=config
有效值	任何批准的插件供应商
默认值	Red Hat, Inc.
语法	DirectoryString
示例	nsslapd-pluginVendor: Red Hat, Inc.

6.1.11. nsslapd-pluginVersion

此属性指定插件版本。

插件参数	描述
条目 DN	cn=plug-in name,cn=plugins,cn=config
有效值	任何有效的插件版本
默认值	产品版本号
语法	DirectoryString
示例	nsslapd-pluginVersion: {VER}

6.2. 某些插件的可选属性

6.2.1. nsslapd-dynamic-plugins

您可以在不重启实例的情况下动态启用一些目录服务器插件。在 Directory Server 中启用 nsslapd-dynamic-plugins 属性以允许动态插件。默认情况下禁用动态插件。

警告

Red Hat Directory Server 不支持动态插件。仅用于测试和调试目的。

您无法将一些插件配置为动态插件。要启用这样的插件，请重启实例。

插件参数	描述
条目 DN	cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-dynamic-plugins: on

6.2.2. nsslapd-pluginConfigArea

有些插件条目是容器条目，插件的多个实例在 cn=plugins,cn=config 中的此容器下创建。但是，cn=plugins,cn=config 没有复制，这意味着必须在每个目录服务器实例上手动配置这些容器条目下的插件配置。

nsslapd-pluginConfigArea 属性指向主数据库区域中的另一个容器条目，其中包含插件实例条目。此容器条目可以位于复制数据库中，允许复制插件配置。

插件参数	描述
条目 DN	cn=*plug-in name*,cn=plugins,cn=config
有效值	任何有效的 DN
默认值	
语法	DN
示例	nsslapd-pluginConfigArea: cn=managed entries container,ou=containers,dc=example,dc=com

6.2.3. nsslapd-plugin-depends-on-named

用于确保服务器以正确顺序调用插件的多值属性。取与插件 cn 值对应的值。此插件之前，服务器将由服务器启动与以下值匹配的 cn 值。如果插件不存在，服务器无法启动。以下 postoperation referential Integrity 插件示例显示了在 Roles 之前启动 Views 插件。如果缺少 Views，服务器将不会启动。

插件参数	描述
条目 DN	cn=referential integrity postoperation,cn=plugins,cn=config
有效值	服务类
默认值	
语法	DirectoryString
示例	* nsslapd-plugin-depends-on-named: Views * nsslapd-pluginId: roles

6.2.4. nsslapd-plugin-depends-on-type

用于确保服务器以正确顺序调用插件的多值属性。取与插件类型对应的值，它包含在 nsslapd-pluginType 属性中。如需更多信息，请参阅 第 6.1.9 节 “nsslapd-pluginType”。所有带有 type 值的插件，与以下有效范围内的其中一个值匹配，服务器将在此插件之前由服务器启动。以下 postoperation referential Integrity 插件示例显示，数据库插件将在 postoperation referential Integrity 插件之前启动。

插件参数	描述
条目 DN	cn=referential integrity postoperation,cn=plugins,cn=config
有效值	database
默认值	
语法	DirectoryString
示例	nsslapd-plugin-depends-on-type: database

6.2.5. nsslapd-pluginLoadGlobal

此属性指定依赖库中的符号是否在本地可见(false)还是可执行文件以及所有共享对象(true)。

插件参数	描述
条目 DN	cn=plug-in name,cn=plugins,cn=config
有效值	true | false
默认值	false
语法	DirectoryString
示例	nsslapd-pluginLoadGlobal: false

6.2.6. nsslapd-pluginLoadNow

此属性指定是否加载插件使用的所有符号（为 ），以及这些符号引用的所有符号，或在第一次使用符号时加载符号(false)。

插件参数	描述
条目 DN	cn=plug-in name,cn=plugins,cn=config
有效值	true | false
默认值	false
语法	DirectoryString
示例	nsslapd-pluginLoadNow: false

6.3. 服务器插件功能参考

本节概述了与 Directory Server 提供的插件，以及其可配置的选项、可配置参数、默认设置、依赖项、常规与性能相关的信息，以及进一步阅读。

6.3.1. 7 位检查插件

插件参数	描述
Plug-in ID	NS7bitAtt
配置条目的 DN	cn=7-bit check,cn=plugins,cn=config
描述	检查某些属性是 7 位清理
类型	preoperation
可配置选项	on | off
默认设置	on
可配置参数	属性列表(**uid mail userpassword**)，后跟 ","，然后后缀进行检查。
依赖项	数据库
性能提升信息	无
更多信息	如果目录服务器使用非 ASCII 字符，如日语，请关闭此插件。

6.3.2. 帐户策略插件

可以设置帐户策略，以便在经过一定时间后自动锁定帐户。这可用于创建仅在预先设置的时间内有效临时帐户，或锁定在一定时间内不活跃的用户。

帐户策略插件本身仅在参数上接受，该参数指向插件配置条目。

```
dn: cn=Account Policy Plugin,cn=plugins,cn=config
...
nsslapd-pluginarg0: cn=config,cn=Account Policy Plugin,cn=plugins,cn=config
```

帐户策略配置条目为整个服务器定义哪些属性用于帐户策略。大多数配置定义了用于评估帐户策略和过期时间的属性，但配置还定义了用来识别子树级别帐户策略定义的对象类。

```
dn: cn=config,cn=Account Policy Plugin,cn=plugins,cn=config
objectClass: top
objectClass: extensibleObject
cn: config

... attributes for evaluating accounts ...
alwaysRecordLogin: yes
stateattrname: lastLoginTime
altstateattrname: createTimestamp

... attributes for account policy entries ...
specattrname: acctPolicySubentry
limitattrname: accountInactivityLimit
```

一个插件被全局配置，帐户策略条目可以在用户子树中创建，然后这些策略可以通过服务类应用到用户和角色。

例 6.1. 帐户策略定义

```
dn: cn=AccountPolicy,dc=example,dc=com
objectClass: top
objectClass: ldapsubentry
objectClass: extensibleObject
objectClass: accountpolicy
# 86400 seconds per day * 30 days = 2592000 seconds
accountInactivityLimit: 2592000
cn: AccountPolicy
```

任何条目（单独的用户和角色）或 CoS 模板可以是帐户策略子条目。每个帐户策略子条目都有一个创建和登录时间，针对任何过期策略进行跟踪。

例 6.2. 具有帐户策略的用户帐户

```
dn: uid=scarter,ou=people,dc=example,dc=com
...
lastLoginTime: 20060527001051Z
acctPolicySubentry: cn=AccountPolicy,dc=example,dc=com
```

插件参数	描述
Plug-in ID	none
配置条目的 DN	cn=Account Policy Plugin,cn=plugins,cn=config
描述	定义在特定过期时间或不活跃的时间后锁定用户帐户的策略。
类型	对象
可配置选项	on | off
默认设置	off
可配置参数	指向包含全局帐户策略设置的配置条目的指针。
依赖项	数据库
性能提升信息	无
更多信息	此插件配置指向一个配置条目，用于帐户不活动和过期数据的服务器端设置。单个(subtree-level 或 user-level)帐户策略可以定义为目录条目，作为 **acctPolicySubentry** 对象类的实例。然后，这些配置条目可以通过服务类应用到用户或角色。

6.3.2.1. altstateattrname

*帐户过期策略基于帐户的一些时间标准。例如，对于不活动策略，主要条件可以是最后的登录时间 **lastLoginTime**。但是，可能存在实例，其中该属性在条目上不存在，例如从未登录其帐户的用户。**altstateattrname** 属性为服务器提供了一个 **backup** 属性，供引用来评估过期时间。*

参数	描述
条目 DN	cn=config,cn=Account Policy Plugin,cn=plugins,cn=config

参数	描述
有效范围	任何基于时间的条目属性
默认值	无
语法	DirectoryString
示例	altstateattrname: createTimeStamp

6.3.2.2. alwaysRecordLogin

默认情况下，只有帐户策略直接应用到它们的条目 - 即，带有 acctPolicySubentry 属性的条目 - 会跟踪其登录时间。如果帐户策略通过服务或角色类别应用，则 acctPolicySubentry 属性位于模板或容器条目上，而不是用户条目本身。

alwaysRecordLogin 属性设置每个条目记录其最后一次登录时间。这允许使用 CoS 和角色来应用帐户策略。

参数	描述
条目 DN	cn=config,cn=Account Policy Plugin,cn=plugins,cn=config
有效范围	是 | 否
默认值	否
语法	DirectoryString
示例	alwaysRecordLogin: no

6.3.2.3. alwaysRecordLoginAttr

Account Policy 插件使用 alwaysRecordLoginAttr 参数中设置的属性名称，将这个属性最后一次成功登录的时间存储在用户的目录条目中。

参数	描述
条目 DN	cn=config,cn=Account Policy Plugin,cn=plugins,cn=config

参数	描述
有效范围	任何有效的属性名称
默认值	stateAttrName
语法	DirectoryString
示例	alwaysRecordLoginAttr: lastLoginTime

6.3.2.4. lastLoginHistSize

要保持成功登录的历史记录，您可以使用 lastLoginHistSize 属性来确定要存储的登录数量，并默认存储最后五次成功登录。

要使 lastLoginHistSize 属性用于存储上次登录，您必须启用 alwaysRecordLogin 属性。

参数	描述
条目 DN	cn=config,cn=Account Policy Plugin,cn=plugins,cn=config
有效范围	0 (disable)到最大 32 位整数值(2147483647)
默认值	5
语法	整数
示例	lastloginhistorysize: 10

6.3.2.5. limitattrname

用户目录中的帐户策略条目定义了帐户锁定策略的时间限制。这个时间限制可以在任何基于时间的属性中设置，策略条目可能会在 ti 中有多个基于时间的属性。策略中用于帐户取消激活限制的属性在 Account Policy Plug-in 的 limitattrname 属性中定义，它被全局应用于所有帐户策略。

参数	描述
条目 DN	cn=config,cn=Account Policy Plugin,cn=plugins,cn=config

参数	描述
有效范围	任何基于时间的条目属性
默认值	无
语法	DirectoryString
示例	limitattrname: accountInactivityLimit

6.3.2.6. specattrname

帐户策略实际上有两个配置条目：插件配置条目中的全局设置，然后在用户目录中的条目中 yser 或 subtree-level 设置。帐户策略可以直接在用户条目上设置，也可以设置为 CoS 或角色配置的一部分。插件识别哪些条目是帐户策略配置条目的方式是识别将其标记为帐户策略的条目上的特定属性。插件配置中的此属性是 specattrname ；它通常设置为 acctPolicySubentry。

参数	描述
条目 DN	cn=config,cn=Account Policy Plugin,cn=plugins,cn=config
有效范围	任何基于时间的条目属性
默认值	无
语法	DirectoryString
示例	specattrname: acctPolicySubentry

6.3.2.7. stateattrname

帐户过期策略基于帐户的一些时间标准。例如，对于不活动策略，主要条件可以是最后的登录时间 lastLoginTime。用于评估帐户策略的主要时间属性在 stateattrname 属性中设置。

参数	描述
条目 DN	cn=config,cn=Account Policy Plugin,cn=plugins,cn=config
有效范围	任何基于时间的条目属性
默认值	无

参数	描述
语法	DirectoryString
示例	stateattrname: lastLoginTime

6.3.3. 帐户 Usability 插件

插件参数	描述
Plug-in ID	acctusability
配置条目的 DN	cn=Account Usability Plugin,cn=plugins,cn=config
描述	检查帐户的身份验证状态或可用性，而无需实际以给定用户身份进行身份验证
类型	preoperation
可配置选项	on | off
默认设置	on
依赖项	数据库
性能提升信息	无

6.3.4. ACL 插件

插件参数	描述
Plug-in ID	acl
配置条目的 DN	cn=ACL Plugin,cn=plugins,cn=config
描述	ACL 访问检查插件
类型	accesscontrol
可配置选项	on | off
默认设置	on
可配置参数	无

插件参数	描述
依赖项	数据库
性能提升信息	访问控制会产生最小性能命中。保持此插件启用，因为它是服务器的访问控制的主要方法。

6.3.5. ACL 抢占插件

插件参数	描述
Plug-in ID	acl
配置条目的 DN	cn=ACL preoperation,cn=plugins,cn=config
描述	ACL 访问检查插件
类型	preoperation
可配置选项	on | off
默认设置	on
可配置参数	无
依赖项	数据库
性能提升信息	访问控制会产生最小性能命中。保持此插件启用，因为它是服务器的访问控制的主要方法。

6.3.6. AD DN 插件

AD DN 插件支持多个域配置。为每个域创建一个配置条目。

插件参数	描述
Plug-in ID	addn
配置条目的 DN	cn=addn,cn=plugins,cn=config
描述	启用使用 Active Directory 格式的用户名，如 ***user_name*** 和 ***user_name@域***，以进行绑定操作。

插件参数	描述
类型	preoperation
可配置选项	on | off
默认设置	off
可配置参数	**addn_default_domain** ：设置默认域，该域会自动附加到没有域的用户名中。
依赖项	无
性能提升信息	无

6.3.6.1. addn_base

设置目录服务器搜索用户 DN 的基本 DN。

参数	描述
条目 DN	cn=*domain_name*,cn=addn,cn=plugins,cn=config
有效的条目	任何有效的 DN
默认值	无
语法	DirectoryString
示例	addn_base: ou=People,dc=example,dc=com

6.3.6.2. addn_filter

设置搜索过滤器。目录服务器自动将 %s 变量替换为身份验证用户的非域部分。例如，如果绑定中的用户名是 user_name@example.com，则过滤器会搜索对应的 DN，其为 (& (objectClass=account) (uid=user_name))。

参数	描述
条目 DN	cn=*domain_name*,cn=addn,cn=plugins,cn=config
有效的条目	任何有效的 DN

参数	描述
默认值	无
语法	DirectoryString
示例	addn_filter: (&(objectClass=account)(uid=%s))

6.3.6.3. cn

设置配置条目的域名。该插件使用身份验证用户名中的域名来选择对应的配置条目。

参数	描述
条目 DN	cn=*domain_name*,cn=addn,cn=plugins,cn=config
有效的条目	任何字符串
默认值	无
语法	DirectoryString
示例	cn: example.com

6.3.7. 别名条目插件

Alias Entries 插件检查对象类 别名 的基本条目，以及包含指向另一个条目的 **DN** 的 **aliasedObjectName** 属性（另一个条目的别名）。在搜索过程中，插件会将搜索基本 **DN** 修改为别名的 **DN**。

Alias Entries 插件仅支持基本级别搜索。使用 **ldapsearch -a find** 命令检索别名的条目。

要使插件返回别名条目，基本条目必须包含以下信息：

- **alias** 对象类。
- **aliasedObjectName** 属性（称为 **X.500** 中的 **aliasedEntryName** 属性），**DN** 值指向另一个条目。

目录服务器可以返回到客户端，并显示以下错误：

- *如果缺少别名 DN，则 错误 32 （没有这样的对象）。*
- *如果搜索 是非基础级搜索，则为 53 错误（不需要执行）。*

解引用是将别名名称转换为对象名称。此过程可能需要检查多个别名条目。别名条目可以指向不是叶条目的条目。DIT 中的条目可能有多个别名名称，多个别名条目可能指向同一条目。

例 6.3. 具有别名的条目

```
dn: cn=Barbara Jensen,ou=Engineering,dc=example,dc=com
objectClass: top
objectClass: alias
objectClass: extensibleObject
cn: Barbara Jensen
aliasedObjectName: cn=Barbara Smith,ou=Engineering,dc=example,dc=com
```

插件参数	描述
Plug-in ID	别名条目
配置条目的 DN	cn=Alias Entries, cn=plugins, cn=config
描述	在 *基本级别* 搜索过程中，检查别名对象类和 **aliasedObjectName** 属性的基本条目
类型	对象
可配置选项	on | off
默认设置	off
可配置参数	别名条目属于 **别名** 对象类。 **aliasedObjectName** 属性存储别名指向的条目的 DN。
依赖项	数据库

插件参数	描述
性能提升信息	每个别名条目都必须属于 **别名** 对象类，并且没有任何子条目。
更多信息	**aliasedObjectName** 属性称为 X.500 中的 **aliasedEntryName** 属性。 **distinguishedNameMatch** 匹配规则和 **DistinguishedName** 语法在 RFC 4517 中定义。

6.3.8. 属性唯一插件

Attribute Uniqueness 插件确保属性值在目录或子树之间是唯一的。

插件参数	描述
Plug-in ID	NSUniqueAttr
配置条目的 DN	cn=Attribute Uniqueness,cn=plugins,cn=config
描述	每次在条目上发生修改时，检查指定属性的值都是唯一的。例如，大多数站点要求用户 ID 和电子邮件地址是唯一的。
类型	preoperation
可配置选项	on | off
默认设置	off
可配置参数	要检查所有列出的子树中的 UID 属性唯一性，请输入 **uid "DN" "DN"...**。但是，要在添加或更新具有 **requiredObjectClass** 的条目时检查 UID 属性唯一性，请输入 **attribute="uid" MarkerObjectclass = "ObjectClassName"**，可选 **requiredObjectClass = "ObjectClassName"**。这将从包含 **MarkerObjectClass** 属性定义的 *ObjectClass* 的父条目开始检查所需的对象类。
依赖项	数据库

插件参数	描述
性能提升信息	目录服务器默认提供 UID 唯一插件。为确保其他属性的唯一值，请为这些属性创建属性插件的实例。 UID 唯一插件默认是 off，因为在多层次复制环境中启用插件前需要解决的操作限制。打开插件可能会减慢目录服务器性能。

6.3.8.1. cn

设置 属性唯一插件配置 记录的名称。您可以使用任何字符串，但红帽建议将配置记录命名为 attribute_name Attribute Uniqueness。

参数	描述
条目 DN	cn=*attribute_uniqueness_configuration_record_name*, cn=plugins,cn=config
有效值	任何有效的字符串
默认值	无
语法	DirectoryString
示例	cn: mail 属性唯一性

6.3.8.2. uniqueness-across-all-subtrees

如果启用(在 上)，插件将检查属性是否在所有子树集中是唯一的。如果将属性设为 off，则仅在更新条目的子树中强制执行唯一性。

参数	描述
条目 DN	cn=*attribute_uniqueness_configuration_record_name*, cn=plugins,cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	uniqueness-across-all-subtrees: off

6.3.8.3. uniqueness-attribute-name

设置值必须是唯一的的属性的名称。此属性是多值。

参数	描述
条目 DN	cn=*attribute_uniqueness_configuration_record_name*, cn=plugins,cn=config
有效值	任何有效的属性名称
默认值	无
语法	DirectoryString
示例	uniqueness-attribute-name: mail

6.3.8.4. uniqueness-subtree-entries-oc

另外，在使用 uniqueness-top-entry-oc 参数时，您可以配置 Attribute Uniqueness 插件，仅验证属性是否是唯一的，如果条目包含此参数中设置的对象类。

参数	描述
条目 DN	cn=*attribute_uniqueness_configuration_record_name*, cn=plugins,cn=config
有效值	任何有效的对象类
默认值	无
语法	DirectoryString
示例	uniqueness-subtree-entries-oc: inetOrgPerson

6.3.8.5. uniqueness-subtrees

设置插件检查属性值的唯一性的 DN。此属性是多值。

参数	描述
条目 DN	cn=*attribute_uniqueness_configuration_record_name*, cn=plugins,cn=config
有效值	任何有效的子树 DN
默认值	无
语法	DirectoryString
示例	uniqueness-subtrees: ou=Sales,dc=example,dc=com

6.3.8.6. uniqueness-top-entry-oc

目录服务器在更新对象的父条目中搜索此对象类。如果没有找到，则搜索将继续进入目录树的根目录。如果找到了对象类，Directory 服务器会验证此子树中 uniqueness-attribute-name 中设置的属性值是否是唯一的。

参数	描述
条目 DN	cn=*attribute_uniqueness_configuration_record_name*, cn=plugins,cn=config
有效值	任何有效的对象类
默认值	无
语法	DirectoryString
示例	uniqueness-top-entry-oc: nsContainer

6.3.9. auto Membership 插件

自动成员规则基本上允许静态组充当动态组。不同的自动成员资格定义创建在所有新目录条目上自动运行的搜索。自动成员规则搜索和识别匹配条目 - 就像动态搜索过滤器 - 相似，然后明确将这些条目作为成员添加到指定的静态组中。

Auto Membership 插件本身是一个容器条目。每个自动成员定义都是 Auto Membership 插件的子项。automember 定义定义 LDAP 搜索基础，并过滤标识条目和默认组以将它们添加到其中。

```
dn: cn=Hostgroups,cn=Auto Membership Plugin,cn=plugins,cn=config
objectclass: autoMemberDefinition
```

```
cn: Hostgroups
autoMemberScope: dc=example,dc=com
autoMemberFilter: objectclass=ipHost
autoMemberDefaultGroup: cn=systems,cn=hostgroups,ou=groups,dc=example,dc=com
autoMemberGroupingAttr: member:dn
```

每个自动成员定义可以有自己的子条目，用于定义将条目分配给组的额外条件。正则表达式可用于包含或排除条目，并根据这些条件将它们分配到特定的组。

```
dn: cn=webservers,cn=Hostgroups,cn=Auto Membership Plugin,cn=plugins,cn=config
objectclass: autoMemberRegexRule
description: Group for webservers
cn: webservers
autoMemberTargetGroup: cn=webservers,cn=hostgroups,dc=example,dc=com
autoMemberInclusiveRegex: fqdn=^www\.web[0-9]+\.example\.com
```

如果条目与主定义匹配，而不是任何正则表达式条件，则它将使用主定义中的组。如果匹配正则表达式条件，则会将其添加到正则表达式条件组中。

插件参数	描述
Plug-in ID	auto Membership
配置条目的 DN	cn=Auto Membership,cn=plugins,cn=config
描述	自动成员规则定义的容器条目。自动成员规则定义搜索新条目，如果它们匹配定义的 LDAP 搜索过滤器和正则表达式条件，则会自动将条目添加到指定的组中。
类型	preoperation
可配置选项	on | off
默认设置	off
可配置参数	none 对于主插件条目。定义条目必须指定 LDAP 范围、LDAP 过滤器、默认组和成员属性格式。可选的正则表达式子条目可以指定 inclusive 和 exclusive 表达式，以及不同的目标组。
依赖项	数据库
性能提升信息	无。

6.3.9.1. autoMemberDefaultGroup

此属性设置 default 或 fallback 组，以将条目作为成员添加到 中。如果只使用定义条目，则这是所有匹配条目的组。如果使用正则表达式条件，如果与 LDAP 搜索过滤器匹配的条目与任何正则表达式不匹配，则此组将用作回退。

参数	描述
条目 DN	cn=Auto Membership Plugin,cn=plugins,cn=config
有效范围	任何现有的 Directory Server 组
默认值	无
单值或多值	单个
语法	DirectoryString
示例	autoMemberDefaultGroup: cn=hostgroups,ou=groups,dc=example,dc=com

6.3.9.2. autoMemberDefinition （对象类）

此属性将条目标识为自动成员定义。此条目必须是 Auto Membership 插件 cn=Auto Membership Plugin,cn=plugins,cn=config 的子级。

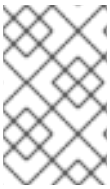
允许的属性

- *autoMemberScope*
- *autoMemberFilter*
- *autoMemberDefaultGroup*
- *autoMemberGroupingAttr*

6.3.9.3. autoMemberExclusiveRegex

此属性设置单一正则表达式，用于识别 要排除的 条目。如果条目与排除条件匹配，则 不会包含在 组中。可以使用多个正则表达式，如果条目与这些表达式中的任何一个匹配，则组中排除了它。

表达式的格式是 Perl 兼容的正则表达式(PCRE)。有关 PCRE 模式的更多信息，请参阅 pcresyntax (3) man page。



注意

排除条件会首先评估，优先于包括条件。

参数	描述
条目 DN	cn=Auto Membership Plugin,cn=plugins,cn=config
有效范围	任何正则表达式
默认值	无
单值或多值	多值
语法	DirectoryString
示例	autoMemberExclusiveRegex: fqdn=^www\.web[0-9]+\.example\.com

6.3.9.4. autoMemberFilter

此属性设置标准 LDAP 搜索过滤器，用于搜索匹配条目。

参数	描述
条目 DN	cn=Auto Membership Plugin,cn=plugins,cn=config
有效范围	任何有效的 LDAP 搜索过滤器
默认值	无
单值或多值	单个
语法	DirectoryString
示例	autoMemberFilter:objectclass=ntUser

6.3.9.5. autoMemberGroupingAttr

此属性提供组条目中 member 属性的名称，以及提供成员属性值的对象条目中的属性，格式为 group_member_attr:entry_attr。

根据组配置，自动成员插件如何将成员添加到组中。例如，对于 groupOfUniqueNames 用户组，每个成员都添加为 uniqueMember 属性。uniqueMember 的值是用户条目的 DN。本质上，每个组成员都由 uniqueMember: user_entry_DN 的 attribute-value 对标识。member 条目格式是 uniqueMember:dn。

参数	描述
条目 DN	cn=Auto Membership Plugin,cn=plugins,cn=config
有效范围	任何目录服务器属性
默认值	无
单值或多值	单个
语法	DirectoryString
示例	autoMemberGroupingAttr: member:dn

6.3.9.6. autoMemberInclusiveRegex

此属性设置单一正则表达式，用于识别要包含 的条目。可以使用多个正则表达式，如果条目与其中一个表达式匹配，它将包含在组中（假设它与 exclude 表达式不匹配）。

表达式的格式是 Perl 兼容的正则表达式(PCRE)。有关 PCRE 模式的更多信息，请参阅 pcresyntax (3) man page。

参数	描述
条目 DN	cn=Auto Membership Plugin,cn=plugins,cn=config
有效范围	任何正则表达式
默认值	无
单值或多值	多值
语法	DirectoryString

参数	描述
示例	autoMemberInclusiveRegex: fqdn=^www\.web[0-9]+\.example\.com

6.3.9.7. autoMemberProcessModifyOps

默认情况下，目录服务器调用 Automembership 插件来添加和修改操作。使用这个设置时，当向用户添加组条目或修改用户的组条目时，插件会更改组。如果将 autoMemberProcessModifyOps 设置为 off，则目录服务器仅在向用户添加组条目时调用 Automembership 插件。在这种情况下，如果管理员更改了用户条目，并且该条目会影响用户所属的 Automembership 组，则插件不会从旧组中删除该用户，仅添加新组。要更新旧组，您必须手动运行修复任务。

参数	描述
条目 DN	cn=Auto Membership Plugin,cn=plugins,cn=config
有效值	on | off
默认值	on
单值或多值	单个
语法	DirectoryString
示例	autoMemberProcessModifyOps: on

6.3.9.8. autoMemberRegexRule （对象类）

此属性将条目标识为正则表达式规则。此条目必须是自动成员定义的子(objectclass: autoMemberDefinition)。

允许的属性

- **autoMemberInclusiveRegex**
- **autoMemberExclusiveRegex**
- **autoMemberTargetGroup**

6.3.9.9. autoMemberScope

此属性设置子树 DN 以搜索条目。这是搜索基础。

参数	描述
条目 DN	cn=Auto Membership Plugin,cn=plugins,cn=config
有效范围	任何目录服务器子树
默认值	无
单值或多值	单个
语法	DirectoryString
示例	autoMemberScope: dc=example,dc=com

6.3.9.10. autoMemberTargetGroup

如果满足正则表达式条件，此属性设置要将条目作为成员添加到 的组。

参数	描述
条目 DN	cn=Auto Membership Plugin,cn=plugins,cn=config
有效范围	任何目录服务器组
默认值	无
单值或多值	单个
语法	DirectoryString
示例	autoMemberTargetGroup: cn=webservers,cn=hostgroups,ou=groups,dc=example,dc=com

6.3.10. 二进制语法插件

警告

二进制语法已弃用。改为使用 Octet 字符串语法。

插件参数	描述
Plug-in ID	bin-syntax
配置条目的 DN	cn=Binary Syntax,cn=plugins,cn=config
描述	处理二进制数据的语法。
类型	syntax
可配置选项	on | off
默认设置	on
可配置参数	无
依赖项	无
性能提升信息	不要修改此插件的配置。红帽建议始终运行此插件。

6.3.11. 位字符串语法插件

插件参数	描述
Plug-in ID	bitstring-syntax
配置条目的 DN	cn=Bit String Syntax,cn=plugins,cn=config
描述	支持来自 RFC 4517 的位字符串语法值和相关匹配规则。
类型	syntax
可配置选项	on | off
默认设置	on

插件参数	描述
可配置参数	无
依赖项	无
性能提升信息	不要修改此插件的配置。红帽建议始终运行此插件。
更多信息	RFC 4517

6.3.12. 位插件

插件参数	描述
Plug-in ID	位
配置条目的 DN	cn=Bitwise Plugin,cn=plugins,cn=config
描述	对 LDAP 服务器执行位操作的匹配规则
类型	matchingrule
可配置选项	on | off
默认设置	on
可配置参数	无
依赖项	无
性能提升信息	不要修改此插件的配置。红帽建议始终运行此插件。

6.3.13. 布尔值语法插件

插件参数	描述
Plug-in ID	boolean-syntax
配置条目的 DN	cn=Boolean Syntax,cn=plugins,cn=config
描述	支持布尔值(TRUE 或 FALSE)以及来自 RFC 4517 的相关匹配规则。
类型	syntax

插件参数	描述
可配置选项	on | off
默认设置	on
可配置参数	无
依赖项	无
性能提升信息	不要修改此插件的配置。红帽建议始终运行此插件。
更多信息	RFC 4517

6.3.14. case Exact String Syntax 插件

插件参数	描述
Plug-in ID	ces-syntax
配置条目的 DN	cn=Case Exact String Syntax,cn=plugins,cn=config
描述	支持区分大小写的匹配或目录字符串、IA5 字符串和相关语法。这不是一个 case-exact 语法；此插件为不同的字符串语法提供区分大小写的匹配规则。
类型	syntax
可配置选项	on | off
默认设置	on
可配置参数	无
依赖项	无
性能提升信息	不要修改此插件的配置。红帽建议始终运行此插件。

6.3.15. case Ignore String Syntax 插件

插件参数	描述
Plug-in ID	directorystring-syntax
配置条目的 DN	cn=Case Ignore String Syntax,cn=plugins,cn=config

插件参数	描述
描述	支持用于目录字符串、IA5 字符串和相关语法的不区分大小写匹配规则。这不是不区分大小写的语法；此插件为不同的字符串语法提供区分大小写的匹配规则。
类型	syntax
可配置选项	on | off
默认设置	on
可配置参数	无
依赖项	无
性能提升信息	不要修改此插件的配置。红帽建议始终运行此插件。

6.3.16. 链数据库插件

插件参数	描述
Plug-in ID	串联数据库
配置条目的 DN	cn=Chaining database,cn=plugins,cn=config
描述	启用链接后端数据库
类型	database
可配置选项	on | off
默认设置	on
可配置参数	无
依赖项	无
性能提升信息	有许多与性能相关的调优参数，它们涉及链数据库。
更多信息	链数据库也称为 *数据库链接*。

6.3.17. Service 插件类

插件参数	描述
Plug-in ID	COS
配置条目的 DN	cn=Class of Service,cn=plugins,cn=config
描述	允许在条目间共享属性
类型	对象
可配置选项	on | off
默认设置	on
可配置参数	无
依赖项	* *类型：* database * *命名：* 状态更改插件 * *named:* Views Plug-in
性能提升信息	不要修改此插件的配置。保持此插件始终运行。

6.3.18. 内容同步插件

插件参数	描述
Plug-in ID	content-sync-plugin
配置条目的 DN	cn=Content Synchronization,cn=plugins,cn=config
描述	根据 RFC 4533，启用对目录服务器中的 **SyncRepl** 协议的支持。
类型	对象
可配置选项	on | off
默认设置	off
可配置参数	无
依赖项	retro Changelog 插件
性能提升信息	如果您知道哪些后端或子树客户端访问来同步数据，请相应地限制 **Retro Changelog** 插件的范围。

6.3.19. Country String Syntax 插件

插件参数	描述
Plug-in ID	countrystring-syntax
配置条目的 DN	cn=Country String Syntax,cn=plugins,cn=config
描述	支持跨国家命名语法值以及来自 RFC 4517 的相关匹配规则。
类型	syntax
可配置选项	on | off
默认设置	on
可配置参数	无
依赖项	无
性能提升信息	不要修改此插件的配置。红帽建议始终运行此插件。
更多信息	RFC 4517

6.3.20. 交付方法语法插件

插件参数	描述
Plug-in ID	delivery-syntax
配置条目的 DN	cn=Delivery Method Syntax,cn=plugins,cn=config
描述	支持值是来自 RFC 4517 的首选交付方法和相关匹配规则的列表。
类型	syntax
可配置选项	on | off
默认设置	on
可配置参数	无
依赖项	无

插件参数	描述
性能提升信息	不要修改此插件的配置。红帽建议始终运行此插件。
更多信息	RFC 4517

6.3.21. deref plug-in

插件参数	描述
Plug-in ID	解引用
配置条目的 DN	cn=deref,cn=plugins,cn=config
描述	在目录搜索中解引用控制
类型	preoperation
可配置选项	on | off
默认设置	on
可配置参数	无
依赖项	数据库
性能提升信息	不要修改此插件的配置。红帽建议始终运行此插件。

6.3.22. 区分名称语法插件

插件参数	描述
Plug-in ID	dn-syntax
配置条目的 DN	cn=Distinguished Name Syntax,cn=plugins,cn=config
描述	支持来自 RFC 4517 的 DN 值语法和相关匹配规则。
类型	syntax
可配置选项	on | off
默认设置	on
可配置参数	无

插件参数	描述
依赖项	无
性能提升信息	不要修改此插件的配置。红帽建议始终运行此插件。
更多信息	RFC 4517

6.3.23. 分布式数字分配插件

分布式数字分配插件管理数字范围，并将该范围内的唯一数字分配给条目。通过将数字分配划分成范围，分布式数字分配插件允许多个服务器分配数字，而不发生冲突。该插件还管理分配给服务器的范围，以便在一个实例通过其范围快速运行时，它可以从其他服务器请求其他范围。

分布式数字分配可以配置为处理单个属性类型或多个属性类型，并且仅应用于子树中的特定后缀和特定条目。

分布式数字分配按属性处理，且仅适用于子树中的特定后缀和特定条目。

插件信息	描述
Plug-in ID	分布式数字分配
配置条目 DN	cn=Distributed Numeric Assignment Plugin,cn=plugins,cn=config
描述	分布式数字分配插件
类型	preoperation
可配置选项	on | off
默认设置	off
可配置参数	
依赖项	数据库
性能提升信息	无

6.3.23.1. dnaFilter

此属性设置一个 LDAP 过滤器，用于搜索和识别要应用分布式数字分配范围的条目。

为属性设置分布式数字分配需要 dnaFilter 属性。

参数	描述
条目 DN	cn=*DNA_config_entry*,cn=Distributed Numeric Assignment Plugin,cn=plugins,cn=config
有效范围	任何有效的 LDAP 过滤器
默认值	无
语法	DirectoryString
示例	dnaFilter: (objectclass=person)

6.3.23.2. dnaHostname

此属性标识共享范围内的服务器的主机名，作为多层次复制中该特定主机的 DNA 范围配置的一部分。可用的范围由主机跟踪，范围信息在所有供应商间复制，以便在任何供应商在可用数字上运行较低时，可以使用主机信息联系另一个供应商并请求新的范围。

参数	描述
条目 DN	cn=*DNA_config_entry*,cn=Distributed Numeric Assignment Plugin,cn=plugins,cn=config
语法	DirectoryString
有效范围	任何有效的主机名
默认值	无
示例	dnahostname: ldap1.example.com

6.3.23.3. dnaInterval

此属性设置一个间隔，用于递增范围中的数字。本质上，这会以预定义的速率跳过数字。如果间隔为 3，且范围中的第一个数字为 1，则范围中使用的下一个数字为 4，然后是 7，然后是 10，每新数字分配增加三。

在复制环境中，dnaInterval 启用多个服务器共享相同的范围。但是，当您配置共享同一范围的不同服务器时，请相应地设置 dnaInterval 和 dnaNextVal 参数，以便不同的服务器不会生成相同的值。如果您在复制拓扑中添加新服务器，还必须考虑这一点。

参数	描述
条目 DN	cn=*DNA_config_entry*,cn=Distributed Numeric Assignment Plugin,cn=plugins,cn=config
有效范围	任何整数
默认值	1
语法	整数
示例	dnaInterval: 1

6.3.23.4. dnaMagicRegen

此属性设置用户定义的值，指示插件为条目分配新值。magic 值可用于为现有条目分配新唯一数字，或者在添加新条目时作为标准设置。

magic 条目应位于服务器的定义范围之外，以便无法被意外触发。请注意，在 DirectoryString 或者其它字符类型中使用时，此属性不必是一个数字。但是，在大多数情形中，DNA 插件用于只接受整数值的属性，在这种情况下，dnamagicregen 值也必须是整数。

参数	描述
条目 DN	cn=*DNA_config_entry*,cn=Distributed Numeric Assignment Plugin,cn=plugins,cn=config
有效范围	任何字符串
默认值	无
语法	DirectoryString
示例	dnaMagicRegen: -1

6.3.23.5. dnaMaxValue

此属性设置可为范围分配的最大值。默认值为 -1， 它与设置最高的 64 位整数相同。

参数	描述
条目 DN	cn=*DNA_config_entry*,cn=Distributed Numeric Assignment Plugin,cn=plugins,cn=config
有效范围	1 到 32 位系统上最大 32 位整数，以及 64 位系统上的最大 64 位整数；-1 代表无限
默认值	-1
语法	整数
示例	dnaMaxValue: 1000

6.3.23.6. dnaNextRange

此属性定义在当前范围耗尽时要使用的下一个范围。这个值会在服务器间传输范围时自动设置，但也可以手动设置将范围添加到服务器（如果没有使用范围请求）。

只有在必须将特定范围分配给其他服务器时，才应明确设置 dnaNextRange 属性。dnaNextRange 属性中设置的任何范围都必须在可用范围内为其他服务器唯一，以避免重复。如果没有来自其他服务器的请求，并且设置了 dnaNextRange 的服务器已明确达到其 set dnaMaxValue，则从此 deck 中分配下一个值（除 dnaNextRange）中。

dnaNextRange 分配也限制在 DNA 配置中设置的 dnaThreshold 属性。为 dnaNextRange 分配给其他服务器的任何范围都无法违反服务器的阈值，即使范围在 dnaNextRange 的 deck 上可用。

注意

如果没有明确设置，如果在内部处理 dnaNextRange 属性。当它被自动处理时，dnaMaxValue 属性充当下一个范围的上限。

属性设置格式为 lower_range-upper_range 的范围。

参数	描述

参数	描述
条目 DN	cn=*DNA_config_entry*,cn=Distributed Numeric Assignment Plugin,cn=plugins,cn=config
有效范围	1 到 32 位系统中最大 32 位整数，以及 64 位系统上用于低和大写的 64 位整数
默认值	无
语法	DirectoryString
示例	dnaNextRange: 100-500

6.3.23.7. dnaNextValue

此属性提供可以分配的下一个可用数字。在最初在配置条目中设置后，此属性由分布式数字分配插件管理。

为属性设置分布式数字分配需要 dnaNextValue 属性。

参数	描述
条目 DN	cn=*DNA_config_entry*,cn=Distributed Numeric Assignment Plugin,cn=plugins,cn=config
有效范围	1 到 32 位系统上最大 32 位整数，以及 64 位系统上的最大 64 位整数
默认值	-1
语法	整数
示例	dnaNextValue: 1

6.3.23.8. dnaPluginConfig （对象类）

此对象类用于配置分配给条目的 DNA 插件和数字范围的条目。

此对象类在 Directory Server 中定义。

优越的类

top

OID

2.16.840.1.113730.3.2.324

允许的属性

- *dnaType*
- *dnaPrefix*
- *dnaNextValue*
- *dnaMaxValue*
- *dnaInterval*
- *dnaMagicRegen*
- *dnaFilter*
- *dnaScope*
- *dnaSharedCfgDN*
- *dnaThreshold*

- *dnaNextRange*
- *dnaRangeRequestTimeout*
- *cn*

6.3.23.9. dnaPortNum

此属性提供用于连接到 dnaHostname 中指定的主机的标准端口号。

参数	描述
条目 DN	cn=*DNA_config_entry*,cn=Distributed Numeric Assignment Plugin,cn=plugins,cn=config
语法	整数
有效范围	0 到 65535
默认值	389
示例	dnaPortNum: 389

6.3.23.10. dnaPrefix

此属性定义一个前缀，可以添加到属性生成的数字值中。例如，要生成用户 ID，如 user1000，dnaPrefix 设置应为 用户。

dnaPrefix 可以保存任何类型的字符串。但是，dnaType （如 uidNumber 和 gidNumber）的一些可能值只需要整数值。要使用前缀字符串，请考虑为 dnaType 使用自定义属性，允许字符串。

参数	描述
条目 DN	cn=*DNA_config_entry*,cn=Distributed Numeric Assignment Plugin,cn=plugins,cn=config
有效范围	任何字符串

参数	描述
默认值	无
示例	dnaPrefix: id

6.3.23.11. dnaRangeRequestTimeout

分布式数字分配插件的一个潜在情况是，一个服务器开始耗尽要分配的数字。dnaThreshold 属性设置范围内可用数字的阈值，以便服务器可以在无法执行编号分配前从其他服务器请求额外的范围。

dnaRangeRequestTimeout 属性为范围请求设置一个超时周期（以秒为单位），以便服务器不会停止等待一个服务器的新范围，并可以从新服务器请求范围。

对于要执行的范围请求，必须设置 dnaSharedCfgDN 属性。

参数	描述
条目 DN	cn=*DNA_config_entry*,cn=Distributed Numeric Assignment Plugin,cn=plugins,cn=config
有效范围	1 到 32 位系统上最大 32 位整数，以及 64 位系统上的最大 64 位整数
默认值	10
语法	整数
示例	dnaRangeRequestTimeout: 15

6.3.23.12. dnaRemainingValues

此属性包含剩余的值数，并可用于分配给条目的服务器。

参数	描述
条目 DN	dnaHostname=*host_name*+dnaPortNum=*port_number*,ou=ranges,dc=example,dc=com
语法	整数

参数	描述
有效范围	任何整数
默认值	无
示例	dnaRemainingValues: 1000

6.3.23.13. dnaRemoteBindCred

指定 Replication Manager 的密码。如果您在需要身份验证的 dnaRemoteBindMethod 属性中设置了 bind 方法，请在 cn=config 条目下为复制部署中的每个服务器设置 dnaRemoteBindCred 参数。

以纯文本设置参数。该值会在存储前自动使用 AES 加密。

需要重新启动服务器才能使更改生效。

参数	描述
条目 DN	cn=*DNA_config_entry*,cn=Distributed Numeric Assignment Plugin,cn=plugins,cn=config
语法	DirectoryString {AES} encrypted_password
有效值	任何有效的 AES 加密密码。
默认值	
示例	dnaRemoteBindCred: {AES-TUhNR0NTcUdTSWIzRFFFRkRUQm1NRVVHQ1NxR1NJYjNEUUVGRERBNEJDUmxObUk0WXpjM1l5MHdaVE5rTXpZNA0KTnkxaEUVGRERBNEJDUmxObUk

6.3.23.14. dnaRemoteBindDN

指定复制管理器 DN。如果您在需要身份验证的 dnaRemoteBindMethod 属性中设置了 bind 方法，请在 cn=config 条目下为复制部署中的每个服务器设置 dnaRemoteBindCred 参数。

需要重新启动服务器才能使更改生效。

参数	描述
条目 DN	cn=*DNA_config_entry*,cn=Distributed Numeric Assignment Plugin,cn=plugins,cn=config
语法	DirectoryString
有效值	任何有效的 Replication Manager DN。
默认值	
示例	dnaRemoteBindDN: cn=replication manager,cn=config

6.3.23.15. dnaRemoteBindMethod

指定远程绑定方法。如果您在需要身份验证的此属性中设置 bind 方法，还要在 cn=config 条目下为复制部署中的每个服务器设置 dnaRemoteBindDN 和 dnaRemoteBindCred 参数。

需要重新启动服务器才能使更改生效。

参数	描述
条目 DN	dnaHostname=*host_name*+dnaPortNum=*port_number*,ou=ranges,dc=example,dc=com
语法	DirectoryString
有效值	**SIMPLE** | **SSL** | **SASL/GSSAPI** | **SASL/DIGEST-MD5**
默认值	
示例	dnaRemoteBindMethod: SIMPLE

6.3.23.16. dnaRemoteConnProtocol

指定远程连接协议。

需要重新启动服务器才能使更改生效。

参数	描述
条目 DN	dnaHostname=*host_name*+dnaPortNum=*port_numbe r*,ou=ranges,dc=example,dc=com
语法	DirectoryString
有效值	**LDAP**、**SSL** 或 **TLS**
默认值	
示例	dnaRemoteConnProtocol: LDAP

6.3.23.17. dnaScope

此属性设置基本 DN，以搜索要应用分布式数字分配的条目。这与 ldapsearch 中的基本 DN 类似。

参数	描述
条目 DN	cn=*DNA_config_entry*,cn=Distributed Numeric Assignment Plugin,cn=plugins,cn=config
有效范围	任何目录服务器条目
默认值	无
语法	DirectoryString
示例	dnaScope: ou=people,dc=example,dc=com

6.3.23.18. dnaSecurePortNum

此属性提供用于连接到 dnaHostname 中指定的主机的安全(TLS)端口号。

参数	描述
条目 DN	dnaHostname=*host_name*+dnaPortNum=*port_numbe r*,ou=ranges,dc=example,dc=com
语法	整数
有效范围	0 到 65535

参数	描述
默认值	636
示例	dnaSecurePortNum: 636

6.3.23.19. dnaSharedCfgDN

此属性定义服务器可用于将范围传输到相互的共享身份。此条目在服务器之间复制，并由插件管理，以便其他服务器知道可用的范围。必须为启用范围传输设置此属性。

注意

共享配置条目必须在复制子树中配置，以便可以将条目复制到服务器。例如，如果复制 ou=People,dc=example,dc=com 子树，则配置条目必须位于该子树中，如 ou=UID Number Ranges,ou=People,dc=example,dc=com。

由此设置标识的条目必须由管理员手动创建。服务器将自动包含其下要传输范围的子条目。

参数	描述
条目 DN	cn=*DNA_config_entry*,cn=Distributed Numeric Assignment Plugin,cn=plugins,cn=config
有效范围	任何 DN
默认值	无
语法	DN
示例	dnaSharedCfgDN: cn=range transfer user,cn=config

6.3.23.20. dnaSharedConfig （对象类）

此对象类用于配置在供应商之间复制的共享配置条目，这些条目全部使用相同的 DNA 插件配置进行数字分配。

此对象类在 Directory Server 中定义。

优越的类

top

OID

2.16.840.1.113730.3.2.325

允许的属性

- **dnaHostname**
- **dnaPortNum**
- **dnaSecurePortNum**
- **dnaRemainingValues**

6.3.23.21. dnaThreshold

分布式数字分配插件的一个潜在情况是，其中一个服务器开始耗尽数字来分配数字，这可能会导致问题。分布式数字分配插件允许服务器从其他服务器上的可用范围请求新范围。

因此，服务器可以在达到其分配范围的末尾识别，因此 dnaThreshold 属性会在范围内设置剩余的可用数字的阈值。当服务器达到阈值时，它会发送新范围的请求。

对于要执行的范围请求，必须设置 dnaSharedCfgDN 属性。

参数	描述
条目 DN	cn=*DNA_config_entry*,cn=Distributed Numeric Assignment Plugin,cn=plugins,cn=config
有效范围	1 到 32 位系统上最大 32 位整数，以及 64 位系统上的最大 64 位整数

参数	描述
默认值	100
语法	整数
示例	dnaThreshold: 100

6.3.23.22. dnaType

此属性设置哪些属性具有为其生成唯一数字。在这种情况下，每当属性通过 magic 数字添加到条目中时，会自动提供分配的值。

为属性设置分布式数字分配需要此属性。

如果设置了 dnaPrefix 属性，则前缀值会添加到 dnaType 生成的任何值前。dnaPrefix 值可以是任意字符串类型，但 dnaType （如 uidNumber 和 gidNumber）的一些合理值只需要整数值。要使用前缀字符串，请考虑为 dnaType 使用自定义属性，允许字符串。

参数	描述
条目 DN	cn=*DNA_config_entry*,cn=Distributed Numeric Assignment Plugin,cn=plugins,cn=config
有效范围	任何目录服务器属性
默认值	无
示例	dnaType: uidNumber

6.3.24. 增强的指南语法插件

插件参数	描述
Plug-in ID	enhancedguide-syntax
配置条目的 DN	cn=Enhanced Guide Syntax,cn=plugins,cn=config
描述	支持基于属性和过滤器创建复杂条件的语法和相关匹配规则，从 RFC 4517 构建搜索。

插件参数	描述
类型	syntax
可配置选项	on | off
默认设置	on
可配置参数	无
依赖项	无
性能提升信息	不要修改此插件的配置。红帽建议始终运行此插件。
更多信息	RFC 4517

6.3.25. Facsimile Telephone Number Syntax 插件

插件参数	描述
Plug-in ID	facsimile-syntax
配置条目的 DN	cn=Facsimile Telephone Number Syntax,cn=plugins,cn=config
描述	支持传真号码的语法和相关匹配规则；来自 RFC 4517。
类型	syntax
可配置选项	on | off
默认设置	on
可配置参数	无
依赖项	无
性能提升信息	不要修改此插件的配置。红帽建议始终运行此插件。
更多信息	RFC 4517

6.3.26. 传真语法插件

插件参数	描述
Plug-in ID	fax-syntax
配置条目的 DN	cn=Fax Syntax,cn=plugins,cn=config
描述	支持语法和相关匹配规则，用于存储传真对象的镜像；来自 RFC 4517。
类型	syntax
可配置选项	on | off
默认设置	on
可配置参数	无
依赖项	无
性能提升信息	不要修改此插件的配置。红帽建议始终运行此插件。
更多信息	RFC 4517

6.3.27. 常规化时间语法插件

插件参数	描述
Plug-in ID	time-syntax
配置条目的 DN	cn=Generalized Time Syntax,cn=plugins,cn=config
描述	支持处理日期、时间和时区的语法和相关匹配规则；来自 RFC 4517。
类型	syntax
可配置选项	on | off
默认设置	on
可配置参数	无
依赖项	无
性能提升信息	不要修改此插件的配置。红帽建议始终运行此插件。

插件参数	描述
更多信息	Generalized Time String 包括四位数、两位月（例如，1 月 1 日）、两位数天、两位数小时、两位数、两位数、两位数秒、一个可选的十进制部分，以及一个时区表示。红帽强烈建议您使用 Z 时区表示 Greenwich Mean Time。 另请参阅 RFC 4517。

6.3.28. 指南语法插件

警告

这个语法已弃用。改为使用 Enhanced Guide 语法。

插件参数	描述
Plug-in ID	guide-syntax
配置条目的 DN	cn=Guide Syntax,cn=plugins,cn=config
描述	基于属性和过滤器创建复杂条件的语法，用于构建搜索
类型	syntax
可配置选项	on | off
默认设置	on
可配置参数	无
依赖项	无
性能提升信息	不要修改此插件的配置。红帽建议始终运行此插件。
更多信息	这个语法已过时。应使用增强的指南语法。

6.3.29. HTTP 客户端插件

插件参数	描述
Plug-in ID	http-client
配置条目的 DN	cn=HTTP Client,cn=plugins,cn=config
描述	HTTP 客户端插件
类型	preoperation
可配置选项	on | off
默认设置	on
可配置参数	无
依赖项	数据库
性能提升信息	

6.3.30. 整数语法插件

插件参数	描述
Plug-in ID	int-syntax
配置条目的 DN	cn=Integer Syntax,cn=plugins,cn=config
描述	支持来自 RFC 4517 的整数语法和相关匹配规则。
类型	syntax
可配置选项	on | off
默认设置	on
可配置参数	无
依赖项	无
性能提升信息	不要修改此插件的配置。红帽建议始终运行此插件。
更多信息	RFC 4517

6.3.31. 国际化插件

插件参数	描述
Plug-in ID	orderingrule
配置条目的 DN	cn=Internationalization Plugin,cn=plugins,cn=config
描述	启用国际化字符串在目录中排序
类型	matchingrule
可配置选项	on | off
默认设置	on
可配置参数	国际插件有一个参数，不得修改该参数，该参数指定 **/etc/dirsrv/config/slapd-collations.conf** 文件的位置。此文件存储国际插件使用的协调顺序和区域。
依赖项	无
性能提升信息	不要修改此插件的配置。红帽建议始终运行此插件。

6.3.32. JPEG 语法插件

插件参数	描述
Plug-in ID	jpeg-syntax
配置条目的 DN	cn=JPEG Syntax,cn=plugins,cn=config
描述	支持 JPEG 镜像数据的语法和相关匹配规则；来自 RFC 4517。
类型	syntax
可配置选项	on | off
默认设置	on
可配置参数	无
依赖项	无
性能提升信息	不要修改此插件的配置。红帽建议始终运行此插件。
更多信息	RFC 4517

6.3.33. ldbm database plug-in

插件参数	描述
Plug-in ID	ldbm-backend
配置条目的 DN	cn=ldbm database,cn=plugins,cn=config
描述	实施本地数据库
类型	database
可配置选项	
默认设置	on
可配置参数	无
依赖项	* 语法 * matchingRule
性能提升信息	有关数据库配置的详情，请查看 第 6.4 节 “数据库插件属性”。

6.3.34. 链接的属性插件

多次，条目彼此之间具有固有的关系（如经理和员工、记录条目及其作者、或特殊组和组成员）。虽然存在反映这些关系的属性，但必须在每个条目上手动添加和更新这些属性。这会导致目录数据集合不一致，其中这些条目关系不明确、过时或缺失。

Linked Attributes Plug-in 允许一个属性（在一个条目中设置）来自动更新另一个条目中的另一个属性。第一个属性具有一个指向要更新的条目的 DN 值；第二个条目属性也具有 DN 值，它是第一个条目的 back-pointer。受用户设置的 link 属性以及受影响条目中的动态更新的"managed"属性都由 Linked Attributes Plug-in 实例中管理员定义。

从概念上讲，这与 MemberOf 插件使用 group 条目中的 member 属性在用户条目中设置 memberOf 属性的方式类似。只有在 Linked 属性插件中，所有 link/managed 属性都是用户定义的，并可有多个插件实例，各自反映不同的链接管理的关系。

链接属性有几个注意事项：

-

link 属性和 managed 属性必须具有 DN 作为值。link 属性中的 DN 指向要向其添加 managed 属性的条目。managed 属性包含链接的条目 DN 作为其值。

- *managed 属性必须是 multi-valued。否则，如果多个链接属性指向同一受管条目，则不会准确更新 managed 属性值。*

插件参数	描述
Plug-in ID	链接的属性
配置条目的 DN	cn=Linked Attributes,cn=plugins,cn=config
描述	链接管理的属性配置条目的容器条目。容器下的每个配置条目都会从一个属性链接到另一个属性，以便在更新一个条目时（如管理器条目），然后与该条目关联的任何条目（如自定义 **directReports** 属性）都会使用用户指定的相应属性自动更新。
类型	preoperation
可配置选项	on | off
默认设置	off
可配置参数	none 对于主插件条目。每个插件实例都有三个可能的属性： * linkType，它为插件设置要监控的主要属性 * managedType，它设置每当修改 linkType 中的属性时由插件动态管理的属性 * linkScope，将插件活动限制为目录树中的特定子树
依赖项	数据库
性能提升信息	linkType 中设置的任何属性都必须只允许 DN 格式的值。managedType 中设置的任何属性都必须是多值。

6.3.34.1. linkScope

这限制了插件的范围，因此它只在特定子树或后缀中运行。如果未指定范围，则插件将更新目录树的任何部分。

参数	描述
条目 DN	cn=*plugin_instance*,cn=Linked Attributes,cn=plugins,cn=config
有效范围	任何 DN
默认值	无
语法	DN
示例	linkScope: ou=People,dc=example,dc=com

6.3.34.2. linkType

这将设置 user-managed 属性。此属性由用户修改和维护，然后在此属性值更改时，目标条目中会自动更新链接的属性。

参数	描述
条目 DN	cn=*plugin_instance*,cn=Linked Attributes,cn=plugins,cn=config
有效范围	任何目录服务器属性
默认值	无
语法	DirectoryString
示例	linkType: directReport

6.3.34.3. managedType

这将设置 managed, 或 插件维护的属性。此属性由 Linked 属性插件实例动态管理。每当对 managed 属性进行更改时，插件会更新目标条目上的所有链接属性。

参数	描述
条目 DN	cn=*plugin_instance*,cn=Linked Attributes,cn=plugins,cn=config
有效范围	任何目录服务器属性

参数	描述
默认值	无
语法	DN
示例	managedType: manager

6.3.35. 受管条目插件

在某些唯一情况下，在创建另一个条目时自动创建条目非常有用。例如，这可以是 Posix 集成的一部分，方法是在创建新用户时创建特定的组条目。Managed Entries 插件的每个实例都标识两个区域：

- ***插件的范围，即子树和搜索过滤器，用于识别需要对应受管条目的条目***
- ***定义受管条目应是什么的模板条目***

插件信息	描述
Plug-in ID	受管条目
配置条目 DN	cn=Managed Entries,cn=plugins,cn=config
描述	自动生成的目录条目的容器条目。每个配置条目都会定义一个目标子树和模板条目。创建目标子树中的匹配条目时，插件会自动基于模板创建新的相关条目。
类型	preoperation
可配置选项	on | off
默认设置	off

插件信息	描述
可配置参数	none 对于主插件条目。每个插件实例都有 4 个可能的属性： * originScope，它设定搜索基础 * originFilter，它为匹配条目设置搜索基础 * managedScope，它设置在其下创建新的受管条目的子树 * managedTemplate，这是用于创建受管条目的模板条目
依赖项	数据库
性能提升信息	无

6.3.35.1. managedBase

此属性设置在其中创建受管条目的子树。这可以是目录树中的任何条目。

参数	描述
条目 DN	cn=*instance_name*,cn=Managed Entries Plugin,cn=plugins,cn=config
有效值	任何目录服务器子树
默认值	无
语法	DirectoryString
示例	managedBase: ou=groups,dc=example,dc=com

6.3.35.2. managedTemplate

此属性标识用于创建受管条目的模板条目。此条目可以位于目录树中的任何位置，但建议此条目位于复制后缀中，以便复制中的所有供应商和消费者都使用相同的模板。

用于创建受管条目模板的属性在 Red Hat Directory Server Configuration, Command, and File Reference 中进行了描述。

参数	描述
条目 DN	cn=*instance_name*,cn=Managed Entries Plugin,cn=plugins,cn=config
有效值	**mepTemplateEntry** 对象类的任何目录服务器条目
默认值	无
语法	DirectoryString
示例	managedTemplate: cn=My Template,ou=Templates,dc=example,dc=com

6.3.35.3. originFilter

此属性设置搜索过滤器，用于搜索和识别需要受管条目的子树中的条目。过滤器允许受管条目行为限制为特定类型的条目或条目子集。语法与常规搜索过滤器相同。

参数	描述
条目 DN	cn=*instance_name*,cn=Managed Entries Plugin,cn=plugins,cn=config
有效值	任何有效的 LDAP 过滤器
默认值	无
语法	DirectoryString
示例	originFilter: objectclass=posixAccount

6.3.35.4. originScope

此属性设置搜索范围，用于查看插件监控的条目。如果在范围子树中创建了新条目，则 Managed Entries 插件会创建一个对应的新受管条目。

参数	描述
条目 DN	cn=*instance_name*,cn=Managed Entries Plugin,cn=plugins,cn=config
有效值	任何目录服务器子树

参数	描述
默认值	无
语法	DirectoryString
示例	originScope: ou=people,dc=example,dc=com

6.3.36. memberOf 插件

组成员资格使用 成员 等属性在组条目内定义。通过搜索 member 属性，可以轻松地列出组的所有成员。但是，组成员资格不会反映在成员的用户条目中，因此无法通过查看用户条目来告知个人所属的组。

MemberOf 插件通过识别组条目中特定成员属性（如成员）的更改，将组成员中的组成员资格与 成员的单个目录条目同步，然后重新写入成员用户条目中的特定属性的成员资格更改。

插件信息	描述
Plug-in ID	memberOf
配置条目 DN	cn=MemberOf Plugin,cn=plugins,cn=config
描述	根据组条目中的成员属性，管理用户条目上的 **memberOf** 属性。
类型	Postoperation
可配置选项	on | off
默认设置	off
可配置参数	* **memberOfAttr** 设置在人员条目中生成的属性，以显示其组成员资格。 * **memberOfGroupAttr** 设置用来识别组成员 DN 的属性。
依赖项	数据库
性能提升信息	无

6.3.36.1. cn

设置插件实例的名称。

参数	描述
条目 DN	cn=MemberOf Plugin,cn=plugins,cn=config
有效值	任何有效的字符串
默认值	
语法	DirectoryString
示例	cn: MemberOf Plugin 实例示例

6.3.36.2. memberOfAllBackends

此属性指定是否为用户条目或所有可用后缀搜索本地后缀。这可以在目录树中实现，在多个数据库中分发用户，以便全面且一致地评估组成员资格。

参数	描述
条目 DN	cn=MemberOf Plugin,cn=plugins,cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	memberOfAllBackends: on

6.3.36.3. memberOfAttr

此属性指定 Directory Server 的用户条目中的属性，用于反映组成员资格。MemberOf 插件为成员的目录条目生成此处指定的属性值。用户所属的每个组都有一个单独的属性。

参数	描述
条目 DN	cn=MemberOf Plugin,cn=plugins,cn=config

参数	描述
有效范围	任何目录服务器属性
默认值	memberOf
语法	DirectoryString
示例	memberOfAttr: memberOf

6.3.36.4. memberOfAutoAddOC

要启用 memberOf 插件向用户添加 memberOf 属性，用户对象必须包含允许此属性的对象类。如果条目没有允许 memberOf 属性的对象类，则 memberOf 插件将自动添加 memberOfAutoAddOC 参数中列出的对象类。

此设置不需要重启服务器才能生效。

参数	描述
条目 DN	cn=MemberOf Plugin,cn=plugins,cn=config
有效值	任何目录服务器对象类
默认值	nsMemberOf
语法	DirectoryString
示例	memberOfAutoAddOC: nsMemberOf

6.3.36.5. memberOfEntryScope

如果您配置了几个后端或多个嵌套后缀，则多值 memberOfEntryScope 参数允许您设置 MemberOf 插件工作的后缀。如果没有设置该参数，则插件可用于所有后缀。memberOfEntryScopeExcludeSubtree 参数中设置的值的优先级高于 memberOfEntryScope 中设置的值。

此设置不需要重启服务器才能生效。

参数	描述
条目 DN	cn=MemberOf Plugin,cn=plugins,cn=config
有效范围	任何目录服务器条目 DN。
默认值	
语法	DirectoryString
示例	memberOfEntryScope: ou=people,dc=example,dc=com

6.3.36.6. memberOfEntryScopeExcludeSubtree

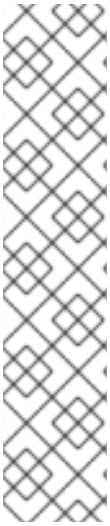
如果您配置了几个后端或多个嵌套后缀，则多值 memberOfEntryScopeExcludeSubtree 参数可让您设置 MemberOf 插件排除的后缀。memberOfEntryScopeExcludeSubtree 参数中设置的值的优先级高于 memberOfEntryScope 中设置的值。如果两个参数中设置的范围重叠，则 MemberOf 插件仅适用于非重叠的目录条目。

此设置不需要重启服务器才能生效。

参数	描述
条目 DN	cn=MemberOf Plugin,cn=plugins,cn=config
有效范围	任何目录服务器条目 DN。
默认值	
语法	DirectoryString
示例	memberOfEntryScopeExcludeSubtree: ou=sample,dc=example,dc=com

6.3.36.7. memberOfGroupAttr

此属性指定组条目中的属性，用于识别组成员的 DN。默认情况下，这是 member 属性，但可以是包含 DN 值的任何成员资格属性，如 uniquemember 或 member。



注意

任何属性都可用于 memberOfGroupAttr 值，但只有 target 属性的值包含成员条目的 DN 时，MemberOf 插件才有效。例如，member 属性包含成员用户条目的 DN：

```
member: uid=jsmith,ou=People,dc=example,dc=com
```

某些与成员相关的属性不包含 DN，如 memberURL 属性。该属性不能作为 memberOfGroupAttr 的值。memberURL 值是一个 URL，非DN 值无法使用 MemberOf 插件。

参数	描述
条目 DN	cn=MemberOf Plugin,cn=plugins,cn=config
有效范围	任何目录服务器属性
默认值	成员
语法	DirectoryString
示例	memberOfGroupAttr: member

6.3.36.8. memberOfSkipNested

如果您没有在目录中使用嵌套组，请将 memberOfSkipNested 属性设置为 on，以跳过嵌套组检查。当目录服务器需要更多的 10000 条目中计算成员资格时，它显著提高更新操作的响应时间。

您不需要重新启动服务器以应用更改。

参数	描述
条目 DN	cn=MemberOf Plugin,cn=plugins,cn=config
有效范围	on | off
默认值	off
语法	DirectoryString
示例	memberOfSkipNested: off

6.3.37. multi-supplier Replication 插件

插件参数	描述
Plug-in ID	replication-multisupplier
配置条目的 DN	cn=Multisupplier Replication Plugin,cn=plugins,cn=config
描述	启用两个当前目录服务器之间的复制
类型	对象
可配置选项	on | off
默认设置	on
可配置参数	无
依赖项	* *named:* ldbm database * *named:* DES * *命名：*服务类
性能提升信息	
更多信息	如果一个服务器永远不会复制，则关闭此插件。

6.3.38. 名称和可选 UID 语法插件

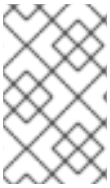
插件参数	描述
Plug-in ID	nameoptuid-syntax
配置条目的 DN	cn=Name and Optional UID Syntax,cn=plugins,cn=config
描述	支持语法和相关匹配规则，以存储和搜索具有可选唯一 ID 的 DN；来自 RFC 4517。
类型	syntax
可配置选项	on | off
默认设置	on

插件参数	描述
可配置参数	无
依赖项	无
性能提升信息	不要修改此插件的配置。红帽建议始终运行此插件。
更多信息	可选 UID 用于区分可能具有相同 DN 或命名属性的条目。 另请参阅 RFC 4517。

6.3.39. 数字字符串语法插件

插件参数	描述
Plug-in ID	numstr-syntax
配置条目的 DN	cn=Numeric String Syntax,cn=plugins,cn=config
描述	支持用于字符串数字和空格的语法和相关匹配规则；来自 RFC 4517。
类型	syntax
可配置选项	on | off
默认设置	on
可配置参数	无
依赖项	无
性能提升信息	不要修改此插件的配置。红帽建议始终运行此插件。
更多信息	RFC 4517

6.3.40. octet String Syntax 插件



注意

使用 Octet String 语法而不是 Binary，它已被弃用。

插件参数	描述
Plug-in ID	octetstring-syntax
配置条目的 DN	cn=Octet String Syntax,cn=plugins,cn=config
描述	支持来自 RFC 4517 的 octet 字符串语法和相关匹配规则。
类型	syntax
可配置选项	on | off
默认设置	on
可配置参数	无
依赖项	无
性能提升信息	不要修改此插件的配置。红帽建议始终运行此插件。
更多信息	RFC 4517

6.3.41. OID 语法插件

插件参数	描述
Plug-in ID	oid-syntax
配置条目的 DN	cn=OID Syntax,cn=plugins,cn=config
描述	支持对象标识符(OID)语法以及 RFC 4517 中相关的匹配规则。
类型	syntax
可配置选项	on | off
默认设置	on
可配置参数	无
依赖项	无
性能提升信息	不要修改此插件的配置。红帽建议始终运行此插件。

插件参数	描述
更多信息	RFC 4517

6.3.42. PAM Pass Through Auth 插件

Unix 系统上的本地 PAM 配置可为 LDAP 用户利用外部身份验证存储。这是直通身份验证的一种形式，允许 Directory 服务器使用外部存储的用户凭证来访问目录。

PAM 直通身份验证是在 PAM Pass Through Auth Plug-in 容器条目下的子条目中配置的。所有可能的配置属性用于 PAM 身份验证（在 60pam-plugin.ldif 架构文件中定义）可用于子条目；子条目必须是 PAM 配置对象类的实例。

例 6.4. PAM Pass Auth 配置条目示例

```
dn: cn=PAM Pass Through Auth,cn=plugins,cn=config
objectClass: top
objectClass: nsSlapdPlugin
objectClass: extensibleObject
objectClass: pamConfig
cn: PAM Pass Through Auth
nsslapd-pluginPath: libpam-passthru-plugin
nsslapd-pluginInitfunc: pam_passthruauth_init
nsslapd-pluginType: preoperation
pass:quotes[nsslapd-pluginEnabled: on]
nsslapd-pluginLoadGlobal: true
nsslapd-plugin-depends-on-type: database
nsslapd-pluginId: pam_passthruauth
nsslapd-pluginVersion: 9.0.0
nsslapd-pluginVendor: Red Hat
nsslapd-pluginDescription: PAM pass through authentication plugin

dn: cn=Example PAM Config,cn=PAM Pass Through Auth,cn=plugins,cn=config
objectClass: top
objectClass: nsSlapdPlugin
objectClass: extensibleObject
objectClass: pamConfig
cn: Example PAM Config
pamMissingSuffix: ALLOW
pass:quotes[pamExcludeSuffix: cn=config]
pass:quotes[pamIDMapMethod: RDN ou=people,dc=example,dc=com]
pass:quotes[pamIDMapMethod: ENTRY ou=engineering,dc=example,dc=com]
pass:quotes[pamIDAttr: customPamUid]
pass:quotes[pamFilter: (manager=uid=bjensen,ou=people,dc=example,dc=com)]
pamFallback: FALSE
pass:quotes[pamSecure: TRUE]
pass:quotes[pamService: ldapserver]
```

在最低程度上，PAM 配置必须定义一个映射方法（确定 PAM 用户 ID 来自 Directory Server 条目）、要使用的 PAM 服务器，以及是否使用安全连接。

```
pamIDMapMethod: RDN
pamSecure: FALSE
pamService: ldapserver
```

可以为特殊设置扩展配置，如排除或专门包含子树，或者将特定属性值映射到 PAM 用户 ID。

插件参数	描述
Plug-in ID	pam_passthruauth
配置条目的 DN	cn=PAM Pass Through Auth,cn=plugins,cn=config
描述	为 PAM 启用直通身份验证，这意味着 PAM 服务可以使用目录服务器作为其用户身份验证存储。
类型	preoperation
可配置选项	on | off
默认设置	on
可配置参数	无
依赖项	数据库
性能提升信息	

6.3.42.1. pamConfig （对象类）

此对象类用于定义与目录服务交互的 PAM 配置。此对象类在 Directory Server 中定义。

优越的类

top

OID

2.16.840.1.113730.3.2.318

允许的属性

- ***pamExcludeSuffix***
- ***pamIncludeSuffix***
- ***pamMissingSuffix***
- ***pamFilter***
- ***pamIDAttr***
- ***pamIDMapMethod***
- ***pamFallback***
- ***pamSecure***
- ***pamService***
- ***nsslapd-pluginConfigArea***

6.3.42.2. pamExcludeSuffix

此属性指定要从 PAM 身份验证中排除的后缀。

OID	2.16.840.1.113730.3.1.2068
语法	DN
multi- 或 Single-Valued	多值

定义在	目录服务器

6.3.42.3. pamFallback

设置在 PAM 身份验证失败时是否回退到常规 LDAP 身份验证。

OID	2.16.840.1.113730.3.1.2072
语法	布尔值
multi- 或 Single-Valued	单值
定义在	目录服务器

6.3.42.4. pamFilter

设置 LDAP 过滤器，用于识别包含的后缀中的特定条目，以使用 PAM 直通身份验证。如果没有设置，则后缀中的所有条目都由配置条目为目标。

OID	2.16.840.1.113730.3.1.2131
语法	布尔值
multi- 或 Single-Valued	单值
定义在	目录服务器

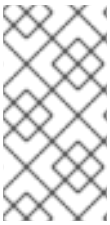
6.3.42.5. pamIDAttr

此属性包含用于存放 PAM 用户 ID 的属性名称。

OID	2.16.840.1.113730.3.1.2071
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	目录服务器

6.3.42.6. pamIDMapMethod

给出将 LDAP 绑定 DN 映射到 PAM 身份的方法。



注意

取消激活目录服务器用户帐户仅使用 ENTRY 映射方法进行验证。使用 RDN 或 DN 时，其帐户处于激活的目录服务器用户仍然可以成功绑定到服务器。

OID	2.16.840.1.113730.3.1.2070
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	目录服务器

6.3.42.7. pamIncludeSuffix

此属性将包含的后缀设置为 PAM 身份验证。

OID	2.16.840.1.113730.3.1.2067
语法	DN
multi- 或 Single-Valued	多值
定义在	目录服务器

6.3.42.8. pamMissingSuffix

标识如何处理缺少的 include 或 exclude 后缀。选项为 ERROR （这会导致 bind 操作失败）；ALLOW，它会记录错误，但允许操作继续进行；IGNORE 允许操作且不记录任何错误。

OID	2.16.840.1.113730.3.1.2069
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	目录服务器

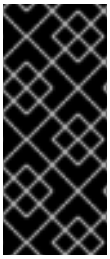
6.3.42.9. pamSecure

需要安全 TLS 连接才能进行 PAM 身份验证。

OID	2.16.840.1.113730.3.1.2073
语法	布尔值
multi- 或 Single-Valued	单值
定义在	目录服务器

6.3.42.10. pamService

包含要传递给 PAM 的服务名称。这假定指定的服务在 /etc/pam.d/ 目录中有一个配置文件。



重要

pam_fprintd.so 模块不能位于 PAM Pass-Through 身份验证插件配置的 pamService 属性引用的配置文件中。使用 PAM pam_fprintd.so 模块会导致目录服务器达到最大文件描述符限制，并可能导致 Directory Server 进程中止。

重要

pam_fprintd.so 模块不能位于 PAM Pass-Through 身份验证插件配置的 pamService 属性引用的配置文件中。使用 PAM fprintd 模块会导致目录服务器达到最大文件描述符限制，并可能导致 Directory 服务器进程中止。

OID	2.16.840.1.113730.3.1.2074
语法	IA5String
multi- 或 Single-Valued	单值
定义在	目录服务器

6.3.43. 透传身份验证插件

插件参数	描述
Plug-in ID	passthruauth
配置条目的 DN	cn=Pass Through Authentication,cn=plugins,cn=config
描述	启用 *直通身份验证*，此机制允许一个目录查阅另一个目录来验证绑定请求。
类型	preoperation
可配置选项	on | off
默认设置	off
可配置参数	ldap://example.com:389/o=example
依赖项	数据库
性能提升信息	直通身份验证会稍微减慢绑定请求，因为它们必须向远程服务器创建额外的跃点。

6.3.44. 密码存储方案

目录服务器将密码存储方案实施为插件。但是，cn=Password 存储 Schemes,cn=plugins,cn=config 条目本身只是一个容器，而不是插件条目。所有密码存储方案插件都作为该容器的子条目存储。

要显示所有密码存储方案插件，请输入：

```
# ldapsearch -D "cn=Directory Manager" -W -H ldap://server.example.com -x \
-b "cn=Password Storage Schemes,cn=plugins,cn=config" -s sub "(objectclass=*)" dn
```

警告

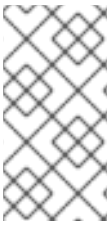
红帽建议不要禁用密码方案插件，也不要更改插件的配置，以防止无法预计的身份验证行为。

强大的密码存储方案

红帽建议只使用以下强大的密码存储方案（最首先）：

- *PBKDF2-SHA512 （默认）。PBKDF2-SHA512 比 PBKDF2_SHA256 更安全。*

基于密码的密钥派生功能 2 (PBKDF2)旨在减少资源以对恶意的强制攻击。PBKDF2 支持变量迭代来应用哈希算法。更高的迭代提高了安全性，但需要更多硬件资源。要应用 PBKDF2-SHA512 算法，目录服务器使用 10,000 迭代。



注意

Red Hat Enterprise Linux 6 中的网络安全服务(NSS)数据库不支持 PBKDF2。因此，您无法在 Directory Server 9 的复制拓扑中使用此密码方案。

- *SSHA512*

salt 的安全哈希算法(SSHA)实施安全哈希算法(SHA)的改进版本，它使用随机生成的 salt 来提高哈希密码的安全性。SSHA512 使用 512 位实施哈希算法。

弱密码存储方案

除了推荐的强密码存储方案外，目录服务器还支持以下弱点方案以向后兼容：

AES	**清除**	**CRYPT**
CRYPT-MD5	**CRYPT-SHA256**	**CRYPT-SHA512**
DES	**MD5**	**NS-MTA-MD5** [a]
SHA [b]	**SHA256**	**SHA384**
SHA512	**SMD5**	**SSHA**
SSHA256	**SSHA384**	

[a] 目录服务器只支持使用此方案进行身份验证。您无法再使用它来加密密码。

[b] 160 位

重要

仅在短时间内继续使用弱方案，因为它会增加安全风险。

6.3.45. POSIX Winsync API 插件

默认情况下，与 Posix 相关的属性不会在 Active Directory 和 {PRODUCT} 之间同步。在 Linux 系统中，系统用户和组被识别为 Posix 条目，LDAP Posix 属性包含该所需信息。但是，当 Windows 用户同步时，它们会自动添加 ntUser 和 ntGroup 属性，将其识别为 Windows 帐户，但没有同步 Posix 属性（即使它们存在于 Active Directory 条目上），也不会在 Directory Server 端添加 Posix 属性。

Posix Winsync API 插件在 Active Directory 和 Directory Server 条目之间同步 POSIX 属性。

注意

所有 POSIX 属性（如 uidNumber、gidNumber 和 homeDirectory）都在 Active Directory 和 Directory Server 条目之间同步。但是，如果将新的 POSIX 条目或 POSIX 属性添加到目录服务器的现有条目中，则只有 POSIX 属性与 Active Directory 对应的条目同步。POSIX 对象类(posixAccount 用于用户，posixGroup 用于组)不会添加到 Active Directory 条目。

此插件默认为禁用，必须在任何 Posix 属性将从 Active Directory 条目同步到 Directory Server 条目前启用。

插件参数	描述
Plug-in ID	posix-winsync-plugin
配置条目的 DN	cn=Posix Winsync API,cn=plugins,cn=config
描述	为 Active Directory 用户和组条目上设置的 Posix 属性启用并配置 Windows 同步。
类型	preoperation

插件参数	描述
可配置参数	* on | off * memberuid 映射(groups) * 在小写（组）中转换并排序 memberUID 值 * memberOf fix-up 任务与同步操作 * 使用 Windows 2003 Posix 模式
默认设置	off
可配置参数	无
依赖项	database

6.3.45.1. posixWinsyncCreateMemberOfTask

此属性设置是否在同步运行后立即运行 memberOf fix-up 任务，以便更新同步用户的组成员资格。这默认是禁用的，因为 memberOf 修复任务可能会大量资源，并在运行太频繁时导致性能问题。

参数	描述
条目 DN	cn=Posix Winsync API Plugin,cn=plugins,cn=config
有效范围	true | false
默认值	false
示例	posixWinsyncCreateMemberOfTask: false

6.3.45.2. posixWinsyncLowerCaseUID

此属性设定是否要在小写的 memberUID 属性中存储（以及转换）UID 值。

参数	描述
条目 DN	cn=Posix Winsync API Plugin,cn=plugins,cn=config
有效范围	true | false
默认值	false

参数	描述
示例	posixWinsyncLowerCaseUID: false

6.3.45.3. posixWinsyncMapMemberUID

此属性设置是否将 Active Directory 组中的 memberUID 属性映射到目录服务器组中的 uniqueMember 属性。

参数	描述
条目 DN	cn=Posix Winsync API Plugin,cn=plugins,cn=config
有效范围	true | false
默认值	true
示例	posixWinsyncMapMemberUID: false

6.3.45.4. posixWinsyncMapNestedGrouping

当 Active Directory POSIX 组中的 memberUID 属性改变时，posixWinsyncMap NestedGrouping 参数会管理。更新嵌套组受到支持 5 级的深度。

参数	描述
条目 DN	cn=Posix Winsync API Plugin,cn=plugins,cn=config
有效范围	true | false
默认值	false
示例	posixWinsyncMapNestedGrouping: false

6.3.45.5. posixWinsyncMsSFUSchema

此属性设置在从 Active Directory 同步 Posix 属性时是否为 Unix 3.0 (msSFU30)模式的旧 Microsoft System Services。默认情况下，Posix Winsync API 插件将 Posix 模式用于现代 Active Directory 服务器：2005、2008 及更新版本。现代 Active Directory Posix 模式与 Windows Server 2003 和较旧的 Windows 服务器使用的 Posix 模式之间存在一些区别。如果 Active Directory 域使用较旧的样式模式，则可以改为使用较早样式的模式。

参数	描述
条目 DN	cn=Posix Winsync API Plugin,cn=plugins,cn=config
有效范围	true | false
默认值	false
示例	posixWinsyncMsSFUSchema: true

6.3.46. 邮政地址字符串语法插件

插件参数	描述
Plug-in ID	postaladdress-syntax
配置条目的 DN	cn=Postal Address Syntax,cn=plugins,cn=config
描述	支持来自 RFC 4517 的邮政地址语法和相关匹配规则。
类型	syntax
可配置选项	on | off
默认设置	on
可配置参数	无
依赖项	无
性能提升信息	不要修改此插件的配置。红帽建议始终运行此插件。
更多信息	RFC 4517

6.3.47. 可打印字符串语法插件

插件参数	描述
Plug-in ID	printablestring-syntax
配置条目的 DN	cn=Printable String Syntax,cn=plugins,cn=config
描述	支持字母数字字符的语法和匹配规则，然后选择标点字符串（字符串符合 RFC 4517 中定义的可打印字符串）。

插件参数	描述
类型	syntax
可配置选项	on | off
默认设置	on
可配置参数	无
依赖项	无
性能提升信息	不要修改此插件的配置。红帽建议始终运行此插件。
更多信息	RFC 4517

6.3.48. 参考完整性插件

插件参数	描述
Plug-in ID	referint
配置条目的 DN	cn=Referential Integrity Postoperation,cn=plugins,cn=config
描述	启用服务器以确保引用完整性
类型	Postoperation
可配置选项	所有配置以及 | off
默认设置	off
可配置参数	启用后相关的引用完整性插件会在删除或重命名操作后立即对 **成员、唯一的成员、所有者和 seeAlso** 属性执行完整性更新。该插件可以配置为对所有其他属性执行完整性检查。
依赖项	数据库
性能提升信息	referential Integrity 插件应在多层次复制环境中的所有供应商上启用。在连锁服务器上启用插件时，请务必分析性能资源和时间需求以及完整性需求；完整性检查可能会花费大量时间，且要求在内存和 CPU 上。指定的所有属性都必须索引，才能同时存在和相等。

6.3.49. retro Changelog 插件

两种不同类型的更改日志由目录服务器维护。第一种类型（称为 更改日志 ）被多层次复制使用，第二个更改日志称为 retro changelog，供 LDAP 客户端用于维护与目录服务器 4.x 版本的兼容性。

这个 Retro Changelog 插件用于记录对供应商服务器的修改。修改供应商服务器的目录时，会将一个条目写入 Retro Changelog 中，其中包含以下任一操作：

- *唯一标识修改的数字。这个数字是与更改日志中的其他条目相关的顺序。*
- *修改操作；即，精确地修改目录。*

它通过 Retro Changelog 插件，通过搜索 cn=changelog 后缀来访问对目录服务器所做的更改。

插件参数	描述
Plug-in ID	retrocl
配置条目的 DN	cn=Retro Changelog Plugin,cn=plugins,cn=config
描述	LDAP 客户端用来维护与目录服务器 4.x 版本的兼容性。维护目录服务器中发生的所有更改的日志。retro changelog 提供了与 Directory Server 4.x 版本中的 changelog 相同的功能。此插件将 **cn=changelog** 后缀公开给客户端，以便客户端可以在没有持久性搜索简单同步应用程序的情况下使用此后缀。
类型	对象
可配置选项	on | off
默认设置	off
可配置参数	有关此插件配置属性的详情，请参考 第 6.3.49 节 “retro Changelog 插件”。
依赖项	* *类型：* database * *命名：* 服务类
性能提升信息	可能会减慢目录服务器更新性能的速度。

6.3.49.1. isReplicated

此可选属性设置一个标志，以指示更改更改是否在该服务器上新做更改，还是将其从其他服务器复制。

参数	描述
OID	2.16.840.1.113730.3.1.2085
条目 DN	cn=Retro Changelog Plugin,cn=plugins,cn=config
有效值	true | false
默认值	无
语法	布尔值
示例	isReplicated: true

6.3.49.2. nsslapd-attribute

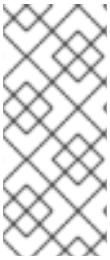
此属性明确指定另一个目录服务器属性，该属性必须包含在 retro changelog 条目中。

许多操作属性和其他类型的属性通常不包括在 retro changelog 中，但可能需要为第三方应用程序提供这些属性以使用 changelog 数据。这可以通过使用 nsslapd-attribute 参数列出 retro changelog 插件配置中的属性。

也可以在 nsslapd-attribute 值中为指定属性指定可选别名。

```
nsslapd-attribute: attribute:pass:attributes[{blank}]alias
```

对属性使用别名可帮助避免与外部服务器或应用程序中的其他属性冲突，这些属性可能会使用 retro changelog 记录。



注意

将 nsslapd-attribute 属性的值设置为 Replicated 是一种 表示方式，在 retro changelog 条目本身中，是否在本地服务器上进行了修改（即，无论更改是原始更改），还是将更改复制到服务器。

参数	描述
条目 DN	cn=Retro Changelog Plugin,cn=plugins,cn=config
有效值	任何有效的目录属性(standard 或 custom)
默认值	无
语法	DirectoryString
示例	nsslapd-attribute: nsUniqueId: uniqueID

6.3.49.3. nsslapd-changelogdir

此属性指定在插件第一次运行时创建 changelog 数据库的目录名称。默认情况下，数据库与 /var/lib/dirsrv/slapd-instance/changelogdb 下的所有其他数据库存储。

注意

出于性能原因，请将此数据库存储在不同的物理磁盘中。

必须重启服务器才能使此属性生效。

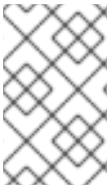
参数	描述
条目 DN	cn=Retro Changelog Plugin,cn=plugins,cn=config
有效值	该目录的任何有效路径
默认值	无
语法	DirectoryString
示例	nsslapd-changelogdir: /var/lib/dirsrv/slapd-*instance*/changelogdb

6.3.49.4. nsslapd-changelogmaxage

nsslapd-changelogmaxage 属性设置 changelog 中任何条目的最长期限。更改日志包含每个目录修改的记录，并在同步消费者服务器时使用。每个记录都包含一个时间戳。任何包含比此属性中指定的值旧

的时间戳的记录都会被删除。默认情况下，Directory 服务器会删除 7 天以上的记录。如果将此属性设置为 0，则对 更改日志没有年龄限制，而目录服务器会保留所有记录。

当您设置较低值时，retro changelog 的大小会自动减少。



注意

如果协议超过最长期限，则不会删除过期的更改记录。

参数	描述
条目 DN	cn=Retro Changelog Plugin,cn=plugins,cn=config
有效范围	0 （表示条目不会根据年龄删除）到最大 32 位整数值 (2147483647)
默认值	7d
语法	DirectoryString *IntegerAgeID*，其中 *AgeID* 是： • **s** (**S**)秒数 • **M** (**M**)表示分钟 • **H** (**H**)小时 • **D**(D)表示天 • **W (W)周** **如果您只设置了不带 *AgeID* 的整数值，则 Directory 服务器将其取为秒。**
示例	nsslapd-changelogmaxage: 30d

6.3.49.5. nsslapd-exclude-attrs

nsslapd-exclude-attrs 参数存储从 retro changelog 数据库中排除的属性名称。要排除多个属性，

请为要排除的每个属性添加一个 nsslapd-exclude-attrs 参数。

参数	描述
条目 DN	cn=Retro Changelog Plugin,cn=plugins,cn=config
有效值	任何有效的属性名称
默认值	无
语法	DirectoryString
示例	nsslapd-exclude-attrs: *example*

6.3.49.6. nsslapd-exclude-suffix

nsslapd-exclude-suffix 参数存储从 retro changelog 数据库中排除的后缀。您可以多次添加参数以排除多个后缀。

参数	描述
条目 DN	cn=Retro Changelog Plugin,cn=plugins,cn=config
有效值	任何有效的属性名称
默认值	无
语法	DirectoryString
示例	nsslapd-exclude-suffix: *ou=demo,dc=example,dc=com*

6.3.50. roles 插件

插件参数	描述
Plug-in ID	roles
配置条目的 DN	cn=Roles Plugin,cn=plugins,cn=config
描述	启用在 Directory 服务器中使用角色
类型	对象

插件参数	描述
可配置选项	on | off
默认设置	on
可配置参数	无
依赖项	* *类型：* database * *命名：* 状态更改插件 * *named:* Views Plug-in
性能提升信息	不要修改此插件的配置。红帽建议始终运行此插件。

6.3.51. rootdn Access Control 插件

root DN cn=Directory Manager 是在普通用户数据库外定义的特殊用户条目。普通的访问控制规则不适用于 root DN，但由于 root 用户强大的性质，将某种访问控制规则应用到 root 用户非常有用。

RootDN 访问控制插件在 root 用户上设置普通访问控制 - 主机和 IP 地址限制、日常限制以及每周天数的限制。

此插件默认为禁用。

插件参数	描述
Plug-in ID	rootdn-access-control
配置条目的 DN	cn=RootDN Access Control,cn=plugins,cn=config
描述	启用并配置用于根 DN 条目的访问控制。
类型	internalpreoperation
可配置选项	on | off
默认设置	off

插件参数	描述
可配置属性	* rootdn-open-time 和 rootdn-close-time 用于基于时间的访问控制 * 基于日常的访问控制的 rootdn-days-allowed * rootdn-allow-host, rootdn-deny-host, rootdn-allow-ip, 和 rootdn-deny-ip 用于基于主机的访问控制
依赖项	无

6.3.51.1. rootdn-allow-host

这会按完全限定的域名设置哪些主机，root 用户被允许用于访问目录服务器。未列出的任何主机都会隐式拒绝。

允许通配符。

此属性可多次使用，以指定多个主机、域或子域。

参数	描述
条目 DN	cn=RootDN Access Control Plugin,cn=plugins,cn=config
有效范围	任何有效的主机名或域，包括通配符的星号 packagemanifests
默认值	无
语法	DirectoryString
示例	rootdn-allow-host: *.example.com

6.3.51.2. rootdn-allow-ip

这会设置哪些 IP 地址，可以是 IPv4 或 IPv6，供 root 用户用于访问目录服务器的机器。没有列出的 IP 地址都会被隐式拒绝。

允许通配符。

此属性可多次使用，以指定多个地址、域或子网。

参数	描述
条目 DN	cn=RootDN Access Control Plugin,cn=plugins,cn=config
有效范围	任何有效的 IPv4 或 IPv6 地址，包括通配符的星号 packagemanifests
默认值	无
语法	DirectoryString
示例	rootdn-allow-ip: 192.168..

6.3.51.3. rootdn-close-time

这会在允许 root 用户访问目录服务器时设置时间段或范围的一部分。当 root 用户不再允许访问目录服务器时，这将设置。

这与 rootdn-open-time 属性一起使用。

参数	描述
条目 DN	cn=RootDN Access Control Plugin,cn=plugins,cn=config
有效范围	任何有效时间，采用 24 小时格式
默认值	无
语法	整数
示例	rootdn-close-time: 1700

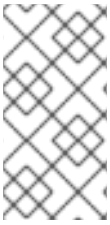
6.3.51.4. rootdn-days-allowed

这提供了允许 root 用户用于访问目录服务器的天数的逗号分隔列表。隐式列出的任何天数都会被拒绝。这可以与 rootdn-close-time 和 rootdn-open-time 一起使用，将基于时间的访问和天-周组合，也可以被自身使用（允许的时间允许的所有小时）。

参数	描述
条目 DN	cn=RootDN Access Control Plugin,cn=plugins,cn=config
有效值	* Sun * mon * Tue * 周三 * 周 * Fri * sat
默认值	无
语法	DirectoryString
示例	rootdn-days-allowed: Mon, Tue, Wed, Thu, Fri

6.3.51.5. rootdn-deny-ip

这为 不允许 root 用户访问目录服务器的机器设置 IP 地址(IPv4 或 IPv6)。没有列出的 IP 地址都会被隐式允许。



注意

拒绝规则 supercede allow 规则，因此如果 rootdn-allow-ip 和 rootdn-deny-ip 属性中都列出了 IP 地址，它将被拒绝访问。

允许通配符。

此属性可多次使用，以指定多个地址、域或子网。

参数	描述
条目 DN	cn=RootDN Access Control Plugin,cn=plugins,cn=config

参数	描述
有效范围	任何有效的 IPv4 或 IPv6 地址，包括通配符的星号 packagemanifests
默认值	无
语法	DirectoryString
示例	rootdn-deny-ip: 192.168.0.0

6.3.51.6. rootdn-open-time

这会在允许 root 用户访问目录服务器时设置时间段或范围的一部分。当基于时间的访问 开始时，此设置。

这与 rootdn-close-time 属性一起使用。

参数	描述
条目 DN	cn=RootDN Access Control Plugin,cn=plugins,cn=config
有效范围	任何有效时间，采用 24 小时格式
默认值	无
语法	整数
示例	rootdn-open-time: 0800

6.3.52. schema Reload 插件

插件信息	描述
Plug-in ID	schemareload
配置条目 DN	cn=Schema Reload,cn=plugins,cn=config
描述	用于重新加载模式文件的任务插件
类型	对象

插件信息	描述
可配置选项	on | off
默认设置	on
可配置参数	无
依赖项	无
性能提升信息	

6.3.53. 空格代表敏感字符串语法插件

插件参数	描述
Plug-in ID	none
配置条目的 DN	cn=Space Insensitive String Syntax,cn=plugins,cn=config
描述	处理空间敏感值的语法
类型	syntax
可配置选项	on | off
默认设置	off
可配置参数	无
依赖项	无
性能提升信息	不要修改此插件的配置。红帽建议始终运行此插件。
更多信息	这个插件可让 Directory 服务器在敏感值 *中支持空间和大小写*。这允许应用程序使用 ASCII 空格字符的条目搜索目录。 例如，如果使用 **jOHN Doe** 的搜索或比较操作将与包含 **johndoe**、john doe、**john doe** 和 **John Doe** 的条目匹配，如果属性的模式已被配置为使用敏感语法中的空格。

6.3.54. 状态更改插件

插件参数	描述
Plug-in ID	statechange
配置条目的 DN	cn=State Change Plugin,cn=plugins,cn=config
描述	启用 state-change-notification 服务
类型	Postoperation
可配置选项	on | off
默认设置	on
可配置参数	无
依赖项	无
性能提升信息	

6.3.55. 语法验证任务插件

插件参数	描述
Plug-in ID	none
配置条目的 DN	cn=Syntax Validation Task,cn=plugins,cn=config
描述	为属性值启用语法验证
类型	对象
可配置选项	on | off
默认设置	on
可配置参数	无
依赖项	无
性能提升信息	
更多信息	此插件实施语法验证任务。执行语法验证的实际进程由每个特定的语法插件执行。

6.3.56. telephone Syntax 插件

插件参数	描述
Plug-in ID	tele-syntax
配置条目的 DN	cn=Telephone Syntax,cn=plugins,cn=config
描述	支持来自 RFC 4517 的电话号码语法和相关匹配规则。
类型	syntax
可配置选项	on | off
默认设置	on
可配置参数	无
依赖项	无
性能提升信息	不要修改此插件的配置。红帽建议始终运行此插件。
更多信息	RFC 4517

6.3.57. Teletex Terminal Identifier Syntax 插件

插件参数	描述
Plug-in ID	teletextermid-syntax
配置条目的 DN	cn=Teletex Terminal Identifier Syntax,cn=plugins,cn=config
描述	支持来自 RFC 4517 的国际电话号码语法和相关匹配规则。
类型	syntax
可配置选项	on | off
默认设置	on
可配置参数	无
依赖项	无

插件参数	描述
性能提升信息	不要修改此插件的配置。红帽建议始终运行此插件。
更多信息	RFC 4517

6.3.58. Telex Number Syntax 插件

插件参数	描述
Plug-in ID	telex-syntax
配置条目的 DN	cn=Telex Number Syntax,cn=plugins,cn=config
描述	支持用于电话号、国家代码和电话端点代码的语法和相关匹配规则；来自 RFC 4517。
类型	syntax
可配置选项	on | off
默认设置	on
可配置参数	无
依赖项	无
性能提升信息	不要修改此插件的配置。红帽建议始终运行此插件。
更多信息	RFC 4517

6.3.59. URI 语法插件

插件参数	描述
Plug-in ID	none
配置条目的 DN	cn=URI Syntax,cn=plugins,cn=config
描述	支持用于唯一资源标识符(URI)的语法和相关匹配规则，包括唯一资源定位器(URL)；来自 RFC 4517。
类型	syntax
可配置选项	on | off

插件参数	描述
默认设置	off
可配置参数	无
依赖项	无
性能提升信息	不要修改此插件的配置。如果启用，红帽建议始终保留此插件运行。
更多信息	RFC 4517

6.3.60. USN 插件

插件参数	描述
Plug-in ID	USN
配置条目的 DN	cn=USN,cn=plugins,cn=config
描述	为每个目录中的每个条目设置更新序列号(USN)，包括添加和删除条目以及修改属性值。
类型	对象
可配置选项	on | off
默认设置	off
可配置参数	无
依赖项	数据库
性能提升信息	对于复制，建议使用部分复制排除 **entryUSN** 配置属性。

6.3.61. 查看插件

插件参数	描述
Plug-in ID	视图
配置条目的 DN	cn=Views,cn=plugins,cn=config

插件参数	描述
描述	在目录服务器数据库中启用视图。
类型	对象
可配置选项	on | off
默认设置	on
可配置参数	无
依赖项	* *类型：* database * *命名：* 状态更改插件
性能提升信息	不要修改此插件的配置。红帽建议始终运行此插件。

6.4. 数据库插件属性

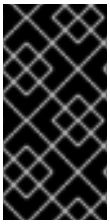
数据库插件也组织在信息树中。数据库实例使用的所有插件技术都存储在 cn=ldbm database 插件节点中。本节以 cn=ldbm database,cn=plugins,cn=config 信息树显示各个节点的额外属性信息。

6.4.1. cn=config,cn=ldbm database,cn=plugins,cn=config 下的数据库属性

本节涵盖所有实例通用的全局配置属性，存储在 cn=config,cn=ldbm database,cn=plugins,cn=config 树节点中。

6.4.1.1. nsslapd-backend-implement

nsslapd-backend-implement 参数定义数据库后端目录服务器使用。



重要

目录服务器目前仅支持 Berkeley 数据库(BDB)。因此，您无法将此参数设置为不同的值。

参数	描述

参数	描述
条目 DN	cn=bdb,cn=config,cn=ldbm database,cn=plugins,cn=config
有效值	bdb
默认值	bdb
语法	目录字符串
示例	nsslapd-backend-implement: bdb

6.4.1.2. nsslapd-backend-opt-level

此参数可触发实验性代码，以提高写入性能。

可能的值：

- 0: 禁用 参数。
- 1： 在事务过程中，复制更新向量不会写入数据库
- 2： 更改获取后端锁定的顺序并启动事务
- 4 ：将代码从事务中移出。

所有参数都可以合并。例如 7 启用所有优化功能。

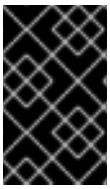
警告

这个参数是实验性的。除非被 红帽支持告知您这样做，否则永远不会更改其值。

参数	描述
条目 DN	cn=config,cn=ldbm database,cn=plugins,cn=config
有效值	0 | 1 | 2 | 4
默认值	0
语法	整数
示例	nsslapd-backend-opt-level: 0

6.4.1.3. nsslapd-db-deadlock-policy

nsslapd-db-deadlock-policy 参数设置 libdb library-internal deadlock 策略。



重要

只有由红帽支持团队指示时才改变此参数。

参数	描述
条目 DN	cn=config,cn=ldbm database,cn=plugins,cn=config
有效值	0-9
默认值	0
语法	DirectoryString
示例	nsslapd-db-deadlock-policy: 9

6.4.1.4. nsslapd-db-private-import-mem

nsslapd-db-private-import-mem 参数管理目录服务器是否使用私有内存来分配区域，以及数据库导入的 mutexes。

参数	描述
条目 DN	cn=config,cn=ldbm database,cn=plugins,cn=config

参数	描述
有效值	on | off
默认值	on
语法	DirectoryString
示例	nsslapd-db-private-import-mem: on

6.4.1.5. nsslapd-db-transaction-wait

如果启用了 nsslapd-db-transaction-wait 参数，Directory 服务器不会启动事务并等待锁定资源可用。

参数	描述
条目 DN	cn=config,cn=ldbm database,cn=plugins,cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-db-transaction-wait: off

6.4.1.6. nsslapd-directory

此属性指定到数据库实例的绝对路径。如果手动创建数据库实例，则必须包含此属性。创建数据库实例后，请勿修改此路径，因为任何更改风险都会阻止服务器访问数据。

参数	描述
条目 DN	cn=config,cn=ldbm database,cn=plugins,cn=config
有效值	数据库实例的任何有效绝对路径
默认值	
语法	DirectoryString

参数	描述
示例	nsslapd-directory: /var/lib/dirsrv/slapd-*instance*/db

6.4.1.7. nsslapd-exclude-from-export

此属性包含导出数据库时要从条目中排除的属性名称列表。这主要用于特定于服务器实例的一些配置和操作属性。

不要删除此属性的任何默认值，因为这可能会影响服务器性能。

参数	描述
条目 DN	cn=config,cn=ldbm database,cn=plugins,cn=config
有效值	任何有效的属性
默认值	entrydn entryid dncomp parentid numSubordinates entryusn
语法	DirectoryString
示例	nsslapd-exclude-from-export: entrydn entryid dncomp parentid numSubordinates entryusn

6.4.1.8. nsslapd-idlistscanlimit

nsslapd-idlistscanlimit 属性已弃用，因为属性对搜索性能的影响比有帮助更有害。进一步描述仅用于历史目的。

这个与性能相关的属性（默认）指定搜索在搜索操作过程中搜索的条目 ID 数量。对于 32 位签名的整数，尝试设置不是数字的值或太大的值会返回 LDAP_UNWILLING_TO_PERFORM 错误消息，以及解释此问题的额外错误信息。建议保留默认值以提高搜索性能。

此参数可以在服务器运行时更改，新值将影响后续搜索。

对应的 user-level 属性是 nsIDListScanLimit。

参数	描述
条目 DN	cn=config,cn=ldbm database,cn=plugins,cn=config
有效范围	100 到最大 32 位整数值(2147483647)条目 ID
默认值	2147483646
语法	整数
示例	nsslapd-idlistscanlimit: 50000

6.4.1.9. nsslapd-idl-switch

nsslapd-idl-switch 参数设置目录服务器使用的 IDL 格式。请注意，红帽不再支持旧的 IDL 格式。

参数	描述
条目 DN	cn=config,cn=ldbm database,cn=plugins,cn=config
有效值	新 | 旧
默认值	new
语法	目录字符串
示例	nsslapd-idl-switch: new

6.4.1.10. nsslapd-lookthroughlimit

此与性能相关的属性指定目录服务器在检查候选条目响应搜索请求时将检查的最大条目数。但是，目录管理器 DN 默认是无限的，并覆盖此处指定的任何其他设置。值得注意的是，基于绑定的资源限制对于这个限制可以正常工作，这意味着如果用户绑定的条目中存在操作属性 nsLookThroughLimit 的值，则默认限制会被覆盖。对于 32 位签名的整数，尝试设置不是数字的值或太大的值会返回 LDAP_UNWILLING_TO_PERFORM 错误消息，以及解释此问题的额外错误信息。

参数	描述
条目 DN	cn=config,cn=ldbm database,cn=plugins,cn=config
有效范围	-1 在条目中最多 32 位整数（其中 -1 代表无限）
默认值	5000

参数	描述
语法	整数
示例	nsslapd-lookthroughlimit: 5000

6.4.1.11. nsslapd-mode

此属性指定用于新创建的索引文件的权限。

参数	描述
条目 DN	cn=config,cn=ldbm database,cn=plugins,cn=config
有效值	任何四位八进制数。但是，建议使用模式 **0600**。这允许对索引文件的所有者（这是运行 **ns-slapd** 的用户）的读写访问权限，其他用户没有访问权限。
默认值	600
语法	整数
示例	nsslapd-mode: 0600

6.4.1.12. nsslapd-pagedidlistscanlimit

此与性能相关的属性指定搜索的条目 ID 数量，特别是使用简单页面的结果控制的搜索操作。

此属性的工作方式与 nsslapd-idlistscanlimit 属性相同，但它只适用于使用简单页面结果控制进行搜索。

如果此属性不存在或设为零，则使用 nsslapd-idlistscanlimit 来分页搜索和非页面搜索。

对应的 user-level 属性是 nsPagedIDListScanLimit。

参数	描述
条目 DN	cn=config,cn=ldbm database,cn=plugins,cn=config

参数	描述
有效范围	-1 在条目中最多 32 位整数（其中 -1 代表无限）
默认值	0
语法	整数
示例	nsslapd-pagedidlistscanlimit: 5000

6.4.1.13. nsslapd-pagedlookthroughlimit

此与性能相关的属性指定目录服务器在检查使用简单页面结果控制的候选条目时检查的最大条目数。

此属性的工作方式与 nsslapd-lookthroughlimit 属性相同，但它只适用于使用简单的页面结果控制进行搜索。

如果此属性不存在或设为零，则使用 nsslapd-lookthroughlimit 来分页搜索和非页面搜索。

对应的 user-level 属性是 nsPagedLookThroughLimit。

参数	描述
条目 DN	cn=config,cn=ldbm database,cn=plugins,cn=config
有效范围	-1 在条目中最多 32 位整数（其中 -1 代表无限）
默认值	0
语法	整数
示例	nsslapd-pagedlookthroughlimit: 25000

6.4.1.14. nsslapd-rangelookthroughlimit

此与性能相关的属性指定目录服务器在检查候选条目响应范围搜索请求时将检查的最大条目数。

范围搜索使用运算符设置括号，以搜索并返回目录中整个条目子集。例如，这会搜索在 1 月 1 日午夜

之后修改的每个条目：

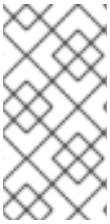
```
(modifyTimestamp>=20200101010101Z)
```

范围搜索的性质是，它必须评估目录中的每一条目，以查看它是否在给定的范围内。基本上，范围搜索始终都是所有 ID 搜索。

对于大多数用户，look-through 限制在 中启动，并防止范围搜索进入所有 ID 搜索。这提高了整体性能，并加快了范围搜索结果。但是，一些客户端或目录管理器等管理用户可能没有设置查找限制。在这种情况下，范围搜索可能需要几分钟才能完成，甚至可以无限期地继续。

nsslapd-rangelookthroughlimit 属性设置适用于所有用户（包括 Directory Manager）的独立范围 look-through 限制。

这允许客户端和管理用户具有高查找限制，同时仍然允许在可能对性能范围搜索上设置合理的限制。



注意

与其他资源限制不同，这适用于任何用户搜索，包括目录管理器、常规用户和其他 LDAP 客户端。

参数	描述
条目 DN	cn=config,cn=ldbm database,cn=plugins,cn=config
有效范围	-1 在条目中最多 32 位整数（其中 -1 代表无限）
默认值	5000
语法	整数
示例	nsslapd-rangelookthroughlimit: 5000

6.4.1.15. nsslapd-search-bypass-filter-test

如果启用了 nsslapd-search-bypass-filter-test 参数，Directory 服务器会在搜索期间构建候选列表时绕过过滤器检查。如果将参数设置为 验证，Directory 服务器会根据搜索候选条目评估过滤器。

参数	描述
条目 DN	cn=config,cn=ldbm database,cn=plugins,cn=config
有效值	on | off | 验证
默认值	on
语法	目录字符串
示例	nsslapd-search-bypass-filter-test: on

6.4.1.16. nsslapd-search-use-vlv-index

nsslapd-search-use-vlv-index 启用和禁用虚拟列表视图(VLV)搜索。

参数	描述
条目 DN	cn=config,cn=ldbm database,cn=plugins,cn=config
有效值	on | off
默认值	on
语法	目录字符串
示例	nsslapd-search-use-vlv-index: on

6.4.2. cn=bdb,cn=config,cn=ldbm database,cn=plugins,cn=config 下的数据库属性

本节涵盖所有实例通用的全局配置属性，存储在 cn=bdb,cn=config,cn=ldbm database,cn=plugins,cn=config 树节点中。

6.4.2.1. nsslapd-cache-autosize

此性能调优相关属性设置总计用于数据库和条目缓存的可用内存百分比。例如，如果值设为 10，则两个缓存都使用系统的可用 RAM 的 10%。如果将此值设置为大于 0 的值，则会为数据库和条目缓存启用自动大小。

为了优化性能，红帽建议不要禁用自动大小。然而，在某些情况下，可能需要禁用自动大小。在这种情况下，将 nsslapd-cache-autosize 属性设置为 0 并手动设置：

- *nsslapd-dbcachesize 属性中的数据库缓存。*
- *nsslapd-cachememsize 属性中的条目缓存。*

注意

如果 nsslapd-cache-autosize 和 nsslapd-cache-autosize-split 属性都被设置为高值，则目录服务器无法启动。要解决这个问题，请将两个参数设置为更合理的值。例如：

```
nsslapd-cache-autosize: 10
nsslapd-cache-autosize-split: 40
```

参数	描述
条目 DN	cn=bdb,cn=config,cn=ldbm database,cn=plugins,cn=config
有效范围	0 到 100。如果设置了 0，则使用默认值。
默认值	10
语法	整数
示例	nsslapd-cache-autosize: 10

6.4.2.2. nsslapd-cache-autosize-split

此性能调优相关属性设置用于数据库缓存的 RAM 百分比。剩余百分比用于条目缓存。例如，如果值设为 40，数据库缓存使用 40%，条目将缓存 nsslapd-cache-autosize 属性中保留的空闲 RAM 的其余 60%。

注意

如果 nsslapd-cache-autosize 和 nsslapd-cache-autosize-split 属性都被设置为高值，则目录服务器无法启动。要解决这个问题，请将两个参数设置为更合理的值。例如：

```
nsslapd-cache-autosize: 10
nsslapd-cache-autosize-split: 40
```

参数	描述
条目 DN	cn=bdb,cn=config,cn=ldbm database,cn=plugins,cn=config
有效范围	0 到 99。如果设置了 0，则使用默认值。
默认值	40
语法	整数
示例	nsslapd-cache-autosize-split: 40

6.4.2.3. nsslapd-dbcachesize

此与性能调整相关的属性指定数据库索引缓存大小（以字节为单位）。这是控制目录服务器使用的物理 RAM 最重要的值之一。

这不是条目缓存。这是 Berkeley 数据库后端将用来缓存索引(.db 文件)和其他文件的内存量。这个值传递给 Berkeley DB API 功能 set_cachesize。如果激活自动缓存大小，服务器会在服务器启动以后的阶段将这些值替换为自己的猜测值时将覆盖此属性。

有关此属性的更多信息，请参阅 link:https://docs.oracle.com/cd/E17076_04/html/programmer_reference/general_am_conf.html#am_conf_cachesize 的 Berkeley DB 参考指南的缓存大小部分。

对于 32 位签名的整数，尝试设置不是数字的值或太大的值会返回 LDAP_UNWILLING_TO_PERFORM 错误消息，以及解释此问题的额外错误信息。

注意

不要手动设置数据库缓存大小。红帽建议使用数据库缓存自动大小功能来优化性能。

必须重启服务器才能使此属性生效。

参数	描述

参数	描述
条目 DN	cn=bdb,cn=config,cn=ldbm database,cn=plugins,cn=config
有效范围	32 位平台 500 KB 到 4GB，64 位平台为 500 KB，64 位平台需要 500 KB 到 2^64-1
默认值	
语法	整数
示例	nsslapd-dbcachesize: 10000000

6.4.2.4. nsslapd-db-checkpoint-interval

这会设置 Directory 服务器向数据库事务日志发送检查点条目的时间（以秒为单位）。数据库事务日志包含所有最近数据库操作的后续列表，仅用于数据库恢复。checkpoint 条目指示已将哪个数据库操作写入目录数据库。checkpoint 条目用于确定数据库事务日志中的位置，以便在系统失败后开始恢复。nsslapd-db-checkpoint-interval 属性没有 dse.ldif。要更改检查点间隔，请将属性添加到 dse.ldif。可以使用 ldapmodify 动态修改此属性。

此属性只提供给系统修改/调优，且仅在红帽技术支持或红帽咨询的指导中更改。此属性的设置不一致，其他配置属性可能会导致 Directory 服务器不稳定。

参数	描述
条目 DN	cn=bdb,cn=config,cn=ldbm database,cn=plugins,cn=config
有效范围	10 到 300 秒
默认值	60
语法	整数
示例	nsslapd-db-checkpoint-interval: 120

6.4.2.5. nsslapd-db-circular-logging

此属性为事务日志文件指定循环日志记录。如果关闭此属性，旧的事务日志文件不会被删除，并被重命名为旧的日志事务文件。关闭循环日志可能会严重降低服务器性能，因此仅应根据红帽技术支持或红帽咨询的指导进行修改。

参数	描述
条目 DN	cn=config,cn=ldbm database,cn=plugins,cn=config
有效值	on | off
默认值	on
语法	DirectoryString
示例	nsslapd-db-circular-logging: on

6.4.2.6. nsslapd-db-debug

此属性指定是否将额外的错误信息报告给目录服务器。要报告错误信息，请在 上将 参数设置为。这个参数用于故障排除；启用参数可能会减慢目录服务器的速度。

参数	描述
条目 DN	cn=config,cn=ldbm database,cn=plugins,cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-db-debug: off

6.4.2.7. nsslapd-db-durable-transactions

此属性设置数据库事务日志条目是否立即写入磁盘。数据库事务日志包含所有最近数据库操作的后续列表，仅用于数据库恢复。启用持久事务后，每个目录更改都会在日志文件中物理记录，因此可在系统失败时恢复。但是，持久化事务功能也可能减慢目录服务器的性能。当禁用持久事务时，所有事务都会在逻辑上写入数据库事务日志中，但可能不会立即写入磁盘。如果在目录更改被物理写入磁盘前出现系统失败，则该更改将无法恢复。nsslapd-db-durable-transactions 属性没有 dse.ldif。要禁用持久事务，请将属性添加到 dse.ldif。

此属性只提供给系统修改/调优，且仅在红帽技术支持或红帽咨询的指导中更改。此属性的设置不一致，其他配置属性可能会导致 Directory 服务器不稳定。

参数	描述
条目 DN	cn=bdb,cn=config,cn=ldbm database,cn=plugins,cn=config
有效值	on | off
默认值	on
语法	DirectoryString
示例	nsslapd-db-durable-transactions: on

6.4.2.8. nsslapd-db-compactdb-interval

nsslapd-db-compactdb-interval 属性定义目录服务器压缩数据库和复制 changelogs 时的时间间隔（以秒为单位）。紧凑操作会将未使用的页面返回到文件系统，数据库文件大小会缩小。请注意，压缩数据库是资源密集型，不应经常完成。

您不必重启服务器才能使此设置生效。

参数	描述
条目 DN	cn=bdb,cn=config,cn=ldbm database,cn=plugins,cn=config
有效值	0 （无压缩）到 2147483647 秒
默认值	2592000 (30 天)
语法	整数
示例	nsslapd-db-compactdb-interval: 2592000

6.4.2.9. nsslapd-db-compactdb-time

nsslapd-db-compactdb-time 属性设置目录服务器压缩所有数据库及其复制更改日志时的时间。超过压缩间隔后运行紧凑任务(nsslapd-db-compactdb-interval)。

您不必重启服务器才能使此设置生效。

参数	描述
条目 DN	cn=bdb,cn=config,cn=ldbm database,cn=plugins,cn=config
有效值	HH:MM.时间设置为 24 小时格式
默认值	23:59
语法	DirectoryString
示例	nsslapd-db-compactdb-time: 23:59

6.4.2.10. nsslapd-db-home-directory

这个参数指定目录服务器数据库的内存映射文件的位置。出于性能原因，此参数的默认值指的是使用 tmpfs 文件系统的 /dev/shm/ 目录。

参数	描述
条目 DN	cn=bdb,cn=config,cn=ldbm database,cn=plugins,cn=config
有效值	任何有效的目录
默认值	/dev/shm/
语法	DirectoryString
示例	nsslapd-db-home-directory: /dev/shm/

6.4.2.11. nsslapd-db-idl-divisor

此属性根据每个数据库页面的块数指定索引块大小。块大小是通过将数据库页面大小除以此属性的值来计算的。值 1 使块大小等于页大小。默认值 0 将块大小设置为页大小减去内部数据库开销的估算允许。对于大多数安装，除非有特定的调优需要，否则不应更改默认值。

在修改此属性的值之前，请使用 db2ldif 脚本导出所有数据库。修改完成后，使用 ldif2db 脚本重新加载数据库。

警告

这个参数应该只供非常高级用户使用。

参数	描述
条目 DN	cn=config,cn=ldbm database,cn=plugins,cn=config
有效范围	0 到 8
默认值	0
语法	整数
示例	nsslapd-db-idl-divisor: 2

6.4.2.12. nsslapd-db-locks

目录服务器中的锁定机制控制目录服务器进程可以同时运行多少个副本。nsslapd-db-locks 参数设置最大锁定数。

只有 Directory 服务器没有锁定并记录 libdb: Lock table is out of available locks 错误信息时，才会将此参数设置为更高的值。如果您在不需要的情况下设置更高的值，这会增加 /var/lib/dirsrv/slapd-instance_name/db_db prerequisites 文件的大小，而无需任何好处。

必须重启该服务才能使此属性生效。

参数	描述
条目 DN	cn=bdb,cn=config,cn=ldbm database,cn=plugins,cn=config
有效范围	0 - 2147483647
默认值	10000
语法	整数

参数	描述
示例	nsslapd-db-locks: 10000

6.4.2.13. nsslapd-db-locks-monitoring-enable

在数据库锁定不足可能会导致数据崩溃。使用 nsslapd-db-locks-monitoring-enable 参数，您可以启用或禁用数据库锁定监控。如果启用了该参数（这是默认设置），如果活跃数据库锁定的数量高于 nsslapd-db-locks-monitoring-threshold 中配置的百分比阈值，则目录服务器会终止所有搜索。如果出现问题，管理员可以在 nsslapd_db_locks 参数中增加数据库锁定的数量。

重启该服务以使更改生效。

参数	描述
条目 DN	cn=bdb,cn=config,cn=ldbm database,cn=plugins,cn=config
有效值	on | off
默认值	on
语法	DirectoryString
示例	nsslapd-db-locks-monitoring-enable: on

6.4.2.14. nsslapd-db-locks-monitoring-pause

如果在 nsslapd-db-locks-monitoring-enable 参数中启用了数据库锁定监控，nsslapd-db-locks-monitoring-pause 定义监控线程在检查之间休眠的时间间隔（毫秒）。

如果将此参数设置为太大的值，服务器可以在监控检查发生前耗尽数据库锁定。但是，设置得太低的值可能会减慢服务器的速度。

您不必重启服务器才能使此设置生效。

参数	描述

参数	描述
条目 DN	cn=bdb,cn=config,cn=ldbm database,cn=plugins,cn=config
有效值	0 - 2147483647 （以毫秒为单位）
默认值	500
语法	DirectoryString
示例	nsslapd-db-locks-monitoring-pause: 500

6.4.2.15. nsslapd-db-locks-monitoring-threshold

如果在 nsslapd-db-locks-monitoring-enable 参数中启用了数据库锁定监控，nsslapd-db-locks-monitoring-threshold 会在 Directory Server 终止搜索前设置使用数据库锁定的最大百分比，以避免进一步锁定耗尽。

重启该服务以使更改生效。

参数	描述
条目 DN	cn=bdb,cn=config,cn=ldbm database,cn=plugins,cn=config
有效值	70 - 95
默认值	90
语法	DirectoryString
示例	nsslapd-db-locks-monitoring-threshold: 90

6.4.2.16. nsslapd-db-logbuf-size

此属性指定日志信息缓冲区大小。日志信息保存在内存中，直到缓冲区填满或事务提交强制将缓冲区写入磁盘。对于长时间运行的事务、高并发应用程序或生成大量数据的事务，更大的缓冲区大小可能会显著提高吞吐量。日志信息缓冲区大小是事务日志大小除以四个分开。

只有在 nsslapd-db-durable-transactions 属性设为 上 时，nsslapd-db-logbuf-size 属性才有效。

参数	描述
条目 DN	cn=bdb,cn=config,cn=ldbm database,cn=plugins,cn=config
有效范围	32k 为最大 32 位整数（限制为机器上可用的内存量）
默认值	32K
语法	整数
示例	nsslapd-db-logbuf-size: 32K

6.4.2.17. nsslapd-db-logdirectory

此属性指定包含数据库事务日志的目录路径。数据库事务日志包含所有最近数据库操作的后续列表。目录服务器在实例意外关闭后使用此信息来恢复数据库。

默认情况下，数据库事务日志存储在与目录数据库相同的目录中。要更新此参数，您必须手动更新 /etc/dirsrv/slapd-instance_name/dse.ldif 文件。

参数	描述
条目 DN	cn=bdb,cn=config,cn=ldbm database,cn=plugins,cn=config
有效值	任何有效的路径
默认值	
语法	DirectoryString
示例	nsslapd-db-logdirectory: /var/lib/dirsrv/slapd-*instance_name*/db/

6.4.2.18. nsslapd-db-logfile-size

此属性指定日志中单个文件的最大大小（以字节为单位）。默认情况下，或者如果值设为 0，则使用最大大小为 10MB。最大大小为未签名的 4 字节值。

参数	描述
条目 DN	cn=config,cn=ldbm database,cn=plugins,cn=config
有效范围	0 到未签名的 4 字节整数
默认值	10MB
语法	整数
示例	nsslapd-db-logfile-size: 10 MB

6.4.2.19. nsslapd-dbncache

此属性可以将 LDBM 缓存分成同样大小的单独内存。可以指定足够大的缓存，以便在某些架构中连续分配它们；例如，有些系统限制进程可能连续分配的内存量。如果 nsslapd-dbncache 是 0 或 1，则缓存将在内存中连续分配。如果它大于 1，缓存将分为 ncache，同样大小独立的内存。

要配置大于 4GB 的 dbcache 大小，请将 nsslapd-dbncache 属性添加到 nsslapd-dbcachesize 和 nsslapd-db-logdirectory 属性行之间的 cn=config,cn=plugins,cn=config。

将此值设置为整数，它是 1-quarter (1/4)的内存量（以 GB 为单位）。例如，对于 12GB 系统，将 nsslapd-dbncache 值设置为 3; 对于 8GB 系统，将其设置为 2。

此属性只为系统修改/调优提供，且仅在红帽技术支持或红帽专业服务的指导中更改。此属性的设置不一致，其他配置属性可能会导致 Directory 服务器不稳定。

必须重启服务器才能使此属性生效。

参数	描述
条目 DN	cn=config,cn=ldbm database,cn=plugins,cn=config
有效值	1 到 4
默认值	1
语法	整数

参数	描述
示例	nsslapd-dbncache: 1

6.4.2.20. nsslapd-db-page-size

此属性指定用于以字节为单位保存数据库的页面大小。最小值为 512 字节，最大大小为 64 KB。如果没有明确设置页大小，Directory 服务器将默认为 8 KB 的页大小。更改此默认值可能会对性能产生显著影响。如果页面大小太小，它会产生大量页面分割和复制，而如果页大小太大，则可能会浪费磁盘空间。

在修改此属性的值之前，请使用 db2ldif 脚本导出所有数据库。修改完成后，使用 ldif2db 脚本重新加载数据库。

参数	描述
条目 DN	cn=config,cn=ldbm database,cn=plugins,cn=config
有效范围	512 字节到 64 KB
默认值	8KB
语法	整数
示例	nsslapd-db-page-size: 8KB

6.4.2.21. nsslapd-db-spin-count

此属性指定 test-and-set mutexes 应该 spin 没有阻塞的次数。

警告

除非您非常熟悉 Berkeley DB 的内部工作，否则永远不会涉及这个值，或者特别告知红帽支持这样做。

默认值 0 可使 BDB 通过多选可用 CPU 内核数（由 nproc 实用程序报告）或 sysconf (_SC_NPROCESSORS_ONLN) 调用来计算 实际值。例如，使用具有 8 个逻辑内核的处理器，将此属性

设置为 0 等同于将其设置为 400。无法完全关闭 - 如果您要最小化 test-and-set mutexes 的次数，如果没有阻止，则将此属性设置为 1。

参数	描述
条目 DN	cn=config,cn=ldbm database,cn=plugins,cn=config
有效范围	0 到 2147483647 (2^31-1)
默认值	0
语法	整数
示例	nsslapd-db-spin-count: 0

6.4.2.22. nsslapd-db-transaction-batch-max-wait

如果设置了 nsslapd-db-transaction-batch-val，则在达到 set batch 值时由单独的线程进行清空。但是，如果只有几个更新，这个过程可能需要很长时间。此参数控制事务应何时独立于批处理计数刷新最新的事务。这些值以毫秒为单位定义。

警告

这个参数是实验性的。除非被 红帽支持告知您这样做，否则永远不会更改其值。

参数	描述
条目 DN	cn=bdb,cn=config,cn=ldbm database,cn=plugins,cn=config
有效范围	0 - 2147483647 （以毫秒为单位）
默认值	50
语法	整数
示例	nsslapd-db-transaction-batch-max-wait: 50

6.4.2.23. nsslapd-db-transaction-batch-min-wait

如果设置了 nsslapd-db-transaction-batch-val，则在达到 set batch 值时由单独的线程进行清空。但是，如果只有几个更新，这个过程可能需要很长时间。这个参数控制事务应最早清除（独立于批处理计数）的时间。这些值以毫秒为单位定义。

警告

这个参数是实验性的。除非被 红帽支持告知您这样做，否则永远不会更改其值。

参数	描述
条目 DN	cn=bdb,cn=config,cn=ldbm database,cn=plugins,cn=config
有效范围	0 - 2147483647 （以毫秒为单位）
默认值	50
语法	整数
示例	nsslapd-db-transaction-batch-min-wait: 50

6.4.2.24. nsslapd-db-transaction-batch-val

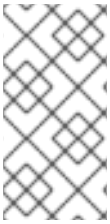
此属性指定提交前将批处理多少个事务。当不需要完整事务持久性时，此属性可以提高更新性能。可以使用 ldapmodify 动态修改此属性。

警告

设置此值将降低数据一致性，并可能导致数据丢失。这是因为，如果服务器在服务器可以清除批处理事务之前出现电源中断，则批处理中的事务将会丢失。

除非被红帽支持特别要求，否则请不要设置这个值。

如果未定义此属性或设置为 0 的值，则会关闭事务批处理，且无法使用 LDAP 对此属性进行远程修改。但是，将此属性设置为大于 0 的值会导致服务器延迟提交事务，直到排队的事务数量等于属性值。大于 0 的值还允许使用 LDAP 远程修改此属性。此属性的 1 值允许使用 LDAP 远程修改属性设置，但不会产生批处理行为。因此，服务器启动时的 1 值对于保持正常持久性非常有用，同时允许在需要时远程打开和关闭事务批处理。请记住，此属性的值可能需要修改 nsslapd-db-logbuf-size 属性，以确保有足够的日志缓冲区大小用于调整批处理的事务。



注意

只有在 nsslapd-db-durable-transaction 属性设置为 上的 nsslapd-db-durable-transaction 属性时，nsslapd-db-transaction-batch-val 属性才有效。

参数	描述
条目 DN	cn=bdb,cn=config,cn=ldbm database,cn=plugins,cn=config
有效范围	0 到 30
默认值	0 （或关闭）
语法	整数
示例	nsslapd-db-transaction-batch-val: 5

6.4.2.25. nsslapd-db-trickle-percentage

此属性设置，在 shared-memory 池中至少指定页面的百分比是通过将脏页面写入其后备文件来清理。这是为了确保页面始终可用于读取新信息，而无需等待写入。

参数	描述
条目 DN	cn=config,cn=ldbm database,cn=plugins,cn=config
有效范围	0 到 100
默认值	40
语法	整数
示例	nsslapd-db-trickle-percentage: 40

6.4.2.26. nsslapd-db-verbose

此属性指定在搜索日志检查点、执行死锁检测和执行恢复时是否记录额外的信息和调试消息。这个参数用于故障排除，启用参数可能会减慢目录服务器的速度。

参数	描述
条目 DN	cn=config,cn=ldbm database,cn=plugins,cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-db-verbose: off

6.4.2.27. nsslapd-import-cache-autosize

这个与性能调整相关的属性会自动将基于命令行的 LDIF 文件导入过程中要使用的导入缓存 (importCache)大小设置为数据库(ldif2db 操作)。

在目录服务器中，导入操作可以作为服务器任务运行，或者只在命令行中运行。在任务模式中，导入操作作为常规目录服务器操作运行。nsslapd-import-cache-autosize 属性启用导入缓存，在导入操作在命令行中运行时自动设置为预先确定的大小。该属性也可以在任务模式导入期间供 Directory 服务器使用，以分配指定百分比的可用内存以导入缓存。

默认情况下，nsslapd-import-cache-autosize 属性被启用，并设置为 -1。这个值只自动调整 ldif2db 操作的导入缓存，自动为导入缓存分配空闲物理内存的五百百分比(50%)。百分比值(50%)被硬编码，不可更改。

将属性值设置为 50 (nsslapd-import-cache-autosize: 50)在 ldif2db 操作期间对性能有同样的效果。但是，当导入操作作为目录服务器任务运行时，此类设置对性能有同样的效果。-1 值自动调整 ldif2db 操作的导入缓存，而不适用于任何，包括导入、常规目录服务器任务。

注意

-1 设置的目的是使 ldif2db 操作能够从空闲物理内存中受益，但同时，不竞争具有条目缓存的宝贵内存，这用于目录服务器的常规操作。

将 nsslapd-import-cache-autosize 属性值设置为 0 可关闭导入缓存自动大小功能 - 也就是说，在导入操作模式中的自动大小不会发生。相反，目录服务器使用 nsslapd-import-cachesize 属性导入缓存大小，默认值为 20000000。

目录服务器上下文中有三个缓存：数据库缓存、条目缓存和导入缓存。导入缓存仅在导入操作期间使用。nsslapd-cache-autosize 属性（用于自动调整条目缓存和数据库缓存）仅在目录服务器操作期间使用，而不在 ldif2db 命令行操作期间使用；属性值是要为条目缓存和数据库缓存分配的空闲物理内存的百分比。

如果自动大小属性，nsslapd-cache-autosize 和 nsslapd-import-cache-autosize 均已启用，请确保其总和小于 100。

参数	描述
条目 DN	cn=bdb,cn=config,cn=ldbm database,cn=plugins,cn=config
有效范围	-1、0 （导入缓存自动大小关闭）到 100
默认值	-1（只为 ldif2db 自动调整导入缓存，并分配 50% 的可用内存来导入缓存）
语法	整数
示例	nsslapd-import-cache-autosize: -1

6.4.2.28. nsslapd-search-bypass-filter-test

如果启用了 nsslapd-search-bypass-filter-test 参数，Directory 服务器会在搜索期间构建候选列表时绕过过滤器检查。如果将参数设置为 验证，Directory 服务器会根据搜索候选条目评估过滤器。

参数	描述
条目 DN	cn=config,cn=ldbm database,cn=plugins,cn=config
有效值	on | off | 验证
默认值	on
语法	目录字符串
示例	nsslapd-search-bypass-filter-test: on

6.4.3. cn=monitor,cn=ldbm database,cn=plugins,cn=config 下的数据库属性

包含监控数据库活动的数据库统计的全局只读属性存储在 cn=monitor,cn=ldbm database,cn=plugins,cn=config 树节点中。

6.4.3.1. currentNormalizedDNcachecount

规范化缓存 DN 的数量。

6.4.3.2. currentNormalizedDNcachesize

规范化 DN 缓存的当前大小（以字节为单位）。

6.4.3.3. dbcachehitratio

此属性显示在数据库缓存中请求页面的百分比(hits/tries)。

6.4.3.4. dbcachehits

此属性显示数据库中找到的请求的页面。

6.4.3.5. dbcachepagein

此属性显示读取到数据库缓存中的页面。

6.4.3.6. dbcachepageout

此属性显示从数据库缓存写入后备文件的页面。

6.4.3.7. dbcacheroevict

此属性显示从缓存中强制的清理页面。

6.4.3.8. dbcacherwevict

此属性显示从缓存中强制脏页面。

6.4.3.9. dbcachetries

此属性显示总缓存查找。

6.4.3.10. maxNormalizedDNcachesize

nsslapd-ndn-cache-max-size 参数的当前值。有关如何更新此设置的详情，请参考 第 2.1.135 节 “nsslapd-ndn-cache-max-size”。

6.4.3.11. normalizedDNcachehitratio

缓存中找到的规范化 DN 的百分比。

6.4.3.12. normalizedDNcachehits

在缓存中找到的规范化 DN。

6.4.3.13. normalizedDNcachemisses

在缓存中未找到规范化 DN。

6.4.3.14. normalizedDNcachetries

自实例启动以来缓存查找的总数。

6.4.4. cn=database_name,cn=ldbm database,cn=plugins,cn=config 下的数据库属性

cn=database_name 子树包含用户定义的数据库的所有配置数据。

默认情况下，cn=userRoot 子树称为 userRoot。但是，这不是硬编码的，假设存在多个数据库实例，因此，用户会更改此名称，并在添加新数据库时由用户定义。引用的 cn=userRoot 数据库可以是任何用户数据库。

以下属性是数据库的通用属性，如 cn=userRoot。

6.4.4.1. nsslapd-cachememsize

此与性能调整相关的属性指定条目缓存的可用内存空间大小（以字节为单位）。最简单的方法是在内存占用方面限制缓存大小。激活自动缓存大小可覆盖此属性，将这些值替换为服务器启动以后的阶段中自己的猜测值。

尝试设置不是数字的值，对于 32 位签名的整数（在 32 位系统中）返回 LDAP_UNWILLING_TO_PERFORM 错误消息，并给出了这个问题的额外错误信息。

此设置的性能计数器最高的 64 位整数，即使在 32 位系统中，但设置本身限制在 32 位系统中，因为系统地址内存的方式限制在 32 位系统中。

注意

不要手动设置数据库缓存大小。红帽建议使用条目缓存自动大小功能来优化性能。

参数	描述
条目 DN	cn=*database_name*,cn=ldbm database,cn=plugins,cn=config
有效范围	64位系统中 500 KB 到 2 64 -1
默认值	209715200 (200 MiB)
语法	整数
示例	nsslapd-cachememsize: 209715200

6.4.4.2. nsslapd-cachesize

此属性已弃用。要重新定义条目缓存大小，请使用 nsslapd-cachememsize。

此性能调优相关属性指定其可保存的条目数的缓存大小。但是，此属性已弃用，而是使用 nsslapd-cachememsize 属性，它为条目缓存大小设置 RAM 绝对分配，如 所述 第 6.4.4.1 节 “nsslapd-cachememsize”

尝试设置不是数字的值，对于 32 位签名的整数（在 32 位系统中）返回 LDAP_UNWILLING_TO_PERFORM 错误消息，并给出了这个问题的额外错误信息。

必须重启服务器才能使此属性生效。

注意

此设置的性能计数器最高的 64 位整数，即使在 32 位系统中，但设置本身限制在 32 位系统中，因为系统地址内存的方式限制在 32 位系统中。

参数	描述
条目 DN	cn=*database_name*,cn=ldbm database,cn=plugins,cn=config
有效范围	在^{32}位系统上 1 到 2 32 -1，或者 64 位系统或 -1 上 2^{63}-1，这意味着无限制
默认值	-1
语法	整数
示例	nsslapd-cachesize: -1

6.4.4.3. nsslapd-directory

此属性指定数据库实例的路径。如果它是一个相对路径，它从全局数据库条目 cn=config,cn=ldbm database,cn=plugins,cn=config 中指定的 nsslapd-directory 指定的路径开始。默认情况下，数据库实例目录以实例名称命名，并默认位于全局数据库目录中。创建数据库实例后，请勿修改此路径，因为任何更改风险都会阻止服务器访问数据。

参数	描述
条目 DN	cn=*database_name*,cn=ldbm database,cn=plugins,cn=config
有效值	数据库实例的任何有效路径
默认值	
语法	DirectoryString

参数	描述
示例	nsslapd-directory: /var/lib/dirsrv/slapd-*instance*/db/userRoot

6.4.4.4. nsslapd-dncachememsize

这个与性能调整相关的属性指定 DN 缓存的可用内存空间大小（以字节为单位）。DN 缓存与数据库的条目缓存类似，只有其表仅存储条目 ID 和条目 DN。这样可以更快地查找重命名和 moddn 操作。

最简单的方法是在内存占用方面限制缓存大小。

尝试设置不是数字的值，对于 32 位签名的整数（在 32 位系统中）返回 LDAP_UNWILLING_TO_PERFORM 错误消息，并给出了这个问题的额外错误信息。

注意

此设置的性能计数器最高的 64 位整数，即使在 32 位系统中，但设置本身限制在 32 位系统中，因为系统地址内存的方式限制在 32 位系统中。

参数	描述
条目 DN	cn=*database_name*,cn=ldbm database,cn=plugins,cn=config
有效范围	^{32}位系统上 500 KB 到 2 32 -1，^{64}位系统上为 2 64 -1
默认值	10,485,760 (10 MB)
语法	整数
示例	nsslapd-dncachememsize: 10485760

6.4.4.5. nsslapd-readonly

此属性为单个后端实例指定只读模式。如果此属性的值为 **off**，则用户具有其访问权限允许的所有读取、写入和执行权限。

参数	描述
条目 DN	cn=*database_name*,cn=ldbm database,cn=plugins,cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-readonly: off

6.4.4.6. nsslapd-require-index

在上切换到时，此属性允许一个拒绝未索引的搜索。此与性能相关的属性可以避免使服务器有错误搜索的饱和。

参数	描述
条目 DN	cn=*database_name*,cn=ldbm database,cn=plugins,cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsslapd-require-index: off

6.4.4.7. nsslapd-require-internalop-index

当插件修改数据时，它在数据库中有一个写入锁定。在大型数据库中，如果插件随后执行未索引的搜索，插件可以使用所有数据库锁定并破坏数据库，或者服务器变得无响应。要避免这个问题，您可以通过启用 **nsslapd-require-internalop-index** 参数来拒绝内部非索引搜索。

参数	描述
条目 DN	cn=*database_name*,cn=ldbm database,cn=plugins,cn=config
有效值	on | off

参数	描述
默认值	off
语法	DirectoryString
示例	nsslapd-require-internalop-index: off

6.4.4.8. nsslapd-suffix

此属性指定 数据库链接 的后缀。这是一个单值属性，因为每个数据库实例只能有一个后缀。在以前的版本中，在单个数据库实例上可以有多个后缀，但这不再是这种情况。因此，此属性是单值来强制实施每个数据库实例只能有一个后缀条目的事实。创建条目后对此属性所做的任何更改仅在重启包含数据库链接的服务器后生效。

参数	描述
条目 DN	cn=*database_name*,cn=ldbm database,cn=plugins,cn=config
有效值	任何有效的 DN
默认值	
语法	DirectoryString
示例	nsslapd-suffix: o=Example

6.4.4.9. vlvBase

此属性设置创建浏览或虚拟列表视图(VLV)索引的基本 DN。

参数	描述
条目 DN	cn=*index_name*,cn=userRoot,cn=ldbm database,cn=plugins,cn=config
有效值	任何有效的 DN
默认值	
语法	DirectoryString

参数	描述
示例	vlvBase: ou=People,dc=example,dc=com

6.4.4.10. vlvEnabled

vlvEnabled 属性提供有关特定 VLV 索引的状态信息，同时目录服务器在运行时设置此属性。虽然 vlvEnabled 显示在配置中，但您无法修改此属性。

参数	描述
条目 DN	cn=*index_name*,cn=userRoot,cn=ldbm database,cn=plugins,cn=config
有效值	0 （禁用）| 1 （启用）
默认值	1
语法	DirectoryString
示例	vlvEnbled: 0

6.4.4.11. vlvFilter

浏览或虚拟列表视图(VLV)索引是通过根据过滤器运行搜索来创建的，并在索引中包含与该过滤器匹配的条目。过滤器在 vlvFilter 属性中指定。

参数	描述
条目 DN	cn=*index_name*,cn=userRoot,cn=ldbm database,cn=plugins,cn=config
有效值	任何有效的 LDAP 过滤器
默认值	
语法	DirectoryString
示例	vlvFilter: (

6.4.4.12. vlvIndex

浏览索引 或虚拟列表视图(VLV)索引 会动态生成条目标头的缩写索引，使其可以更快地浏览大型索引。VLV 索引定义有两个部分：一个定义索引，另一个定义用于标识要添加到索引的搜索。vlvIndex 对象类定义索引条目。

此对象类在 Directory Server 中定义。

优越的类

top

OID

2.16.840.1.113730.3.2.42

表 6.2. 必要属性

属性	定义
objectClass	定义条目的对象类。
cn	提供条目的通用名称。
vlvSort	标识浏览索引（虚拟列表视图索引）是否排序的属性列表。

表 6.3. 允许的属性

属性	定义
vlvEnabled	存储浏览索引的可用性。
vlvUses	包含使用浏览索引的数量。

6.4.4.13. vlvScope

此属性设置搜索范围，以针对浏览或虚拟列表视图(VLV)索引中的条目运行。

参数	描述
条目 DN	cn=*index_name*,cn=userRoot,cn=ldbm database,cn=plugins,cn=config

参数	描述
有效值	* 1 （一级或子项搜索） * 2 (subtree search)
默认值	
语法	整数
示例	vlvScope: 2

6.4.4.14. vlvSearch

浏览索引 或虚拟列表视图(VLV)索引 会动态生成条目标头的缩写索引，使其可以更快地浏览大型索引。VLV 索引定义有两个部分：一个定义索引，另一个定义用于标识要添加到索引的搜索。vlvSearch 对象类定义搜索过滤器条目。

此对象类在 Directory Server 中定义。

优越的类

top

OID

2.16.840.1.113730.3.2.38

表 6.4. 必要属性

属性	定义
objectClass	定义条目的对象类。
vlvBase	标识创建浏览索引的基本 DN。
vlvScope	标识定义浏览索引的范围。
vlvFilter	标识用于定义浏览索引的过滤器字符串。

表 6.5. 允许的属性

属性	定义
multiLineDescription	提供条目的文本描述。

6.4.4.15. vlvSort

此属性设置浏览或虚拟列表视图(VLV)索引中返回的条目的排序顺序。

注意

此属性的条目是 vlvSearch 条目下的 vlvIndex 条目。

参数	描述
条目 DN	cn=*index_name*,cn=*index_name*,cn=userRoot,cn=ldbm database,cn=plugins,cn=config
有效值	任何目录服务器属性，在以空格分隔的列表中
默认值	
语法	DirectoryString
示例	vlvSort: cn givenName o ou sn

6.4.4.16. vlvUses

vlvUses 属性包含浏览索引使用的数量，Directory 服务器在运行时设置此属性。虽然 vlvUses 显示在配置中，但您无法修改此属性。

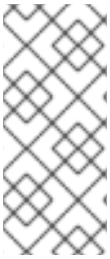
参数	描述
条目 DN	cn=*index_name*,cn=userRoot,cn=ldbm database,cn=plugins,cn=config
有效值	N/A
默认值	
语法	DirectoryString

参数	描述
示例	vlvUses: 800

6.4.5. cn=database,cn=monitor,cn=ldbm database,cn=plugins,cn=config 下的数据库属性

此树节点条目中的属性都是只读、数据库性能计数器。这些属性的所有值为 32 位整数，但 entrycachehits 和 entrycachetries 除外。

如果在 上将 cn=config 中的 nsslapd-counters 属性设为 on，则目录服务器实例会递增使用 64 位整数，即使 32 位机器或 32 位目录服务器版本。对于数据库监控，entrycachehits 和 entrycachetries 计数器使用 64 位整数。



注意

nsslapd-counters 属性为这些特定的数据库和服务器计数器启用 64 位支持。使用 64 位整数的计数器不可配置；所有允许的计数器都启用了 64 位整数，或为所有允许的计数器禁用。

6.4.5.1. currentdncachecount

此属性显示当前在 DN 缓存中存在的 DN 数量。

6.4.5.2. currentdncachesize

此属性显示 DN 缓存中当前存在的总大小（以字节为单位）。

6.4.5.3. maxdncachesize

此属性显示可在数据库 DN 缓存中维护的 DN 的最大大小（以字节为单位）。

6.4.5.4. nsslapd-db-abort-rate

此属性显示已中止的事务数。

6.4.5.5. nsslapd-db-active-txns

此属性显示当前活跃的事务数。

6.4.5.6. nsslapd-db-cache-hit

此属性显示缓存中找到的请求的页面。

6.4.5.7. nsslapd-db-cache-region-wait-rate

此属性显示在获取区域锁定前强制等待的控制线程等待的次数。

6.4.5.8. nsslapd-db-cache-size-bytes

此属性显示总缓存大小（以字节为单位）。

6.4.5.9. nsslapd-db-cache-try

此属性显示总缓存查找。

6.4.5.10. nsslapd-db-clean-pages

此属性显示当前在缓存中的清理页面。

6.4.5.11. nsslapd-db-commit-rate

此属性显示已提交的事务数。

6.4.5.12. nsslapd-db-deadlock-rate

此属性显示检测到的死锁数量。

6.4.5.13. nsslapd-db-dirty-pages

此属性显示当前在缓存中的脏页面。

6.4.5.14. nsslapd-db-hash-buckets

此属性显示缓冲区哈希表中的散列 bucket 数量。

6.4.5.15. nsslapd-db-hash-elements-examine-rate

此属性显示在哈希表查找过程中遍历的哈希元素总数。

6.4.5.16. nsslapd-db-hash-search-rate

此属性显示缓冲区哈希表查找的总数。

6.4.5.17. nsslapd-db-lock-conflicts

此属性显示因为冲突而不能立即可用的锁定总数。

6.4.5.18. nsslapd-db-lockers

此属性显示当前锁定器的数量。

6.4.5.19. nsslapd-db-lock-region-wait-rate

此属性显示在获取区域锁定前强制等待的控制线程等待的次数。

6.4.5.20. nsslapd-db-lock-request-rate

此属性显示请求的锁定总数。

6.4.5.21. nsslapd-db-log-bytes-since-checkpoint

此属性显示自上次检查点以来写入此日志的字节数。

6.4.5.22. nsslapd-db-log-region-wait-rate

此属性显示在获取区域锁定前强制等待的控制线程等待的次数。

6.4.5.23. nsslapd-db-log-write-rate

此属性显示写入此日志的 MB 和字节数。

6.4.5.24. nsslapd-db-longest-chain-length

此属性显示在缓冲区哈希表查找中遇到的最长链。

6.4.5.25. nsslapd-db-page-create-rate

此属性显示缓存中创建的页面。

6.4.5.26. nsslapd-db-page-read-rate

此属性显示读取到缓存中的页面。

6.4.5.27. nsslapd-db-page-ro-evict-rate

此属性显示从缓存中强制的清理页面。

6.4.5.28. nsslapd-db-page-rw-evict-rate

此属性显示从缓存中强制脏页面。

6.4.5.29. nsslapd-db-pages-in-use

此属性显示当前正在使用的所有页面、干净或脏页面。

6.4.5.30. nsslapd-db-page-trickle-rate

此属性显示使用 memp_trickle 接口编写的脏页面。

6.4.5.31. nsslapd-db-page-write-rate

此属性显示读取到缓存中的页面。

6.4.5.32. nsslapd-db-txn-region-wait-rate

此属性显示控制线程在获取区域锁定前等待的次数。

6.4.6. cn=changelog,cn=database_name,cn=ldbm database,cn=plugins,cn=config 下的数据库属性

在多层次复制中，Directory 服务器将 changelog 配置条目存储在 cn=changelog,cn=database_name,cn=ldbm database,cn=plugins,cn=config 条目中，其具有 top 和 extensibleObject 对象类。

注意

术语 更改日志 可能会参考：

变更日志

使用本章中描述的属性的多层次复制中的实际更改日志。

retro Changelog

Directory 服务器用来与某些传统应用程序兼容的插件。如需更多信息，请参阅 第 6.3.49 节 “retro Changelog 插件”。

6.4.6.1. cn

cn 属性设置 changelog 条目的相对可分辨名称(RDN)。此属性是必需的。

参数	描述
条目 DN	cn=changelog,cn=*database_name*,cn=ldbm database,cn=plugins,cn=config
有效值	任何字符串
默认值	changelog
语法	DirectoryString
示例	cn=changelog,cn=userRoot,cn=ldbm database,cn=plugins

6.4.6.2. nsslapd-changelogcompactdb-interval

nsslapd-changelogcompactdb-interval 属性定义目录服务器压缩复制 changelogs 时的时间间隔（以秒为单位）。紧凑操作会将未使用的页面返回到文件系统，数据库文件大小会缩小。请注意，压缩数据库是资源密集型，您不得经常这样做。

您不需要重新启动服务器以应用属性值更改。

参数	描述
条目 DN	n=changelog,cn=database_name,cn=ldbm database,cn=plugins,cn=config
有效值	0 （无压缩）到 2147483647 秒
默认值	2592000 (30 天)
语法	整数
示例	nsslapd-changelogcompactdb-interval: 2592000

6.4.6.3. nsslapd-changelogmaxage

与消费者同步时，目录服务器将每个更新存储在更改日志中，并带有一个时间戳。nsslapd-changelogmaxage 属性设置存储在 changelog 中的记录的最大年龄。目录服务器会自动删除成功传输到所有消费者的旧记录。默认情况下，Directory 服务器会删除 7 天以上的记录。但是，如果您禁用了 nsslapd-changelogmaxage 和 nsslapd-changelogmaxentries 属性，Directory 服务器会将所有记录保留在更改日志中，并可能导致 changelog 文件的过度增长。

注意

retro changelog 具有自己的 nsslapd-changelogmaxage 属性。如需更多信息，请参阅 Retro changelog nsslapd-changelogmaxage

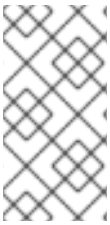
目录服务器以 nsslapd-changelogtrim-interval 属性中设置的间隔执行修剪操作。

您必须重启服务器以应用属性值更改。

参数	描述
条目 DN	cn=changelog,cn=*database_name*,cn=ldbm database,cn=plugins,cn=config
有效范围	0 （条目不会根据其年龄删除）到最大 32 位整数 (2147483647)
默认值	7d
语法	DirectoryString *IntegerAgeID*，其中 *AgeID* 是： • **s** (**S**)秒数 • **M** (**M**)表示分钟 • **H** (**H**)小时 • **D**(D)表示天 • **W (W)周** **如果您只设置了不带 *AgeID* 的整数值，则 Directory 服务器将其取为秒。**
示例	nsslapd-changelogmaxage: 30d

6.4.6.4. nsslapd-changelogmaxentries

nsslapd-changelogmaxentries 属性设置更改日志中存储的最大记录数。如果成功传输到所有消费者的最旧的记录数量超过 nsslapd-changelogmaxentries 值，Directory 服务器会自动从 changelog 中删除这些记录。如果将 nsslapd-changelogmaxentries 和 nsslapd-changelogmaxage 属性设置为 0，则目录服务器会将所有记录保留在 changelog 中，这可能会导致 changelog 文件的过度增长。



注意

如果您在 nsslapd-changelogmaxentries 属性中设置了较低值，则目录服务器不会自动缩小复制 changelog 的文件大小。

目录服务器以 nsslapd-changelogtrim-interval 属性中设置的间隔执行修剪操作。

您必须重启服务器以应用属性值更改。

参数	描述
条目 DN	cn=changelog,cn=*database_name*,cn=ldbm database,cn=plugins,cn=config
有效范围	0 （唯一最大限制是磁盘大小）到最大 32 位整数 (2147483647)
默认值	0
语法	整数
示例	nsslapd-changelogmaxentries: 5000

6.4.6.5. nsslapd-changelogtrim-interval

目录服务器会在 changelog 上重复运行修剪进程。要更改两个运行之间的时间，请更新 nsslapd-changelogtrim-interval 属性并设置间隔（以秒为单位）。

您不需要重新启动服务器以应用属性更改。

参数	描述
条目 DN	cn=changelog,cn=*database_name*,cn=ldbm database,cn=plugins,cn=config
有效范围	0 到最大 32 位整数值(2147483647)
默认值	300 (5 分钟)
语法	DirectoryString
示例	nsslapd-changelogtrim-interval: 300

6.4.6.6. nsslapd-encryptionalgorithm

nsslapd-encryptionalgorithm 属性指定用于更改日志加密的加密算法 Directory 服务器。要启用更改日志加密，您必须在目录服务器中安装服务器证书。

您必须重启服务器以应用属性值更改。

参数	描述
条目 DN	cn=changelog,cn=*database_name*,cn=ldbm database,cn=plugins,cn=config
有效范围	AES 或 3DES
默认值	无
语法	DirectoryString
示例	nsslapd-encryptionalgorithm: AES

6.4.6.7. nsSymmetricKey

nsSymmetricKey 属性存储内部生成的对称密钥。

您必须重启服务器以应用属性值更改。

参数	描述
条目 DN	cn=changelog,cn=*database_name*,cn=ldbm database,cn=plugins,cn=config
有效范围	base64 编码的密钥
默认值	无
语法	DirectoryString
示例	无

6.4.7. cn=monitor,cn=database_name,cn=ldbm database,cn=plugins,cn=config 下的数据库属性

此树节点条目中的属性都是只读、数据库性能计数器。

如果在 上将 cn=config 中的 nsslapd-counters 属性设为 on，则目录服务器实例会递增使用 64 位整数，即使 32 位机器或 32 位目录服务器版本。对于数据库监控，entrycachehits 和 entrycachetries 计数器使用 64 位整数。

注意

nsslapd-counters 属性为这些特定的数据库和服务器计数器启用 64 位支持。使用 64 位整数的计数器不可配置；所有允许的计数器都启用了 64 位整数，或为所有允许的计数器禁用。

6.4.7.1. currentDNcachecount

缓存的 DN 数。

6.4.7.2. currentDNcachesize

以字节为单位的 DN 缓存的当前大小。

6.4.7.3. dbfilecachehit-number

此属性给出了搜索需要执行此文件数据的次数，并且数据从缓存中成功获取。此属性名称中的数字对应于 dbfilename 中的数字。

6.4.7.4. dbfilecachemiss-number

此属性给出了搜索需要执行此文件数据的次数，并且无法从缓存中获取数据。此属性名称中的数字对应于 dbfilename 中的数字。

6.4.7.5. dbfilename-number

此属性提供文件的名称，并为文件提供连续的整数标识符（从 0 开始）。文件的所有关联统计信息将给出同样的数字标识符。

6.4.7.6. dbfilepagein-number

此属性提供从此文件传递给缓存的页面数量。此属性名称中的数字对应于 dbfilename 中的数字。

6.4.7.7. dbfilepageout-number

此属性提供此文件从缓存写入到磁盘的页面数。此属性名称中的数字对应于 dbfilename 中的数字。

6.4.7.8. DNcachehitratio

缓存中找到的 DN 的百分比。

6.4.7.9. DNcachehits

在缓存中找到的 DNS。

6.4.7.10. DNcachemisses

在缓存中未找到 DNS。

6.4.7.11. DNcachetries

自实例启动以来缓存查找的总数。

6.4.7.12. maxDNcachesize

nsslapd-ndn-cache-max-size 参数的当前值。有关如何更新此设置的详情，请参考 第 2.1.135 节 “nsslapd-ndn-cache-max-size”。

6.4.8. cn=default index,cn=config,cn=ldbm database,cn=plugins,cn=config 下的数据库属性

默认索引集合存储在此处。默认索引为每个后端配置，以便为大多数设置场景优化目录服务器功能。除系统必要的索引外，所有索引都可以被删除，但应谨慎处理，因为不会造成不必要的中断。

6.4.8.1. cn

此属性提供要索引的属性的名称。

参数	描述
条目 DN	cn=default indexes,cn=config,cn=ldbm database,cn=plugins,cn=config
有效值	任何有效的索引 cn
默认值	无
语法	DirectoryString
示例	cn: aci

6.4.8.2. nsIndex

此对象类在后端数据库中定义索引。此对象在 Directory Server 中定义。

优越的类

top

OID

2.16.840.1.113730.3.2.44

表 6.6. 必要属性

属性	定义
objectClass	定义条目的对象类。
cn	提供条目的通用名称。
nsSystemIndex	确定索引是否为系统定义的索引。

表 6.7. 允许的属性

属性	定义
description	提供条目的文本描述。
nsIndexType	标识索引类型。

属性	定义
nsMatchingRule	标识匹配的规则。

6.4.8.3. nsIndexType

此可选的多值属性指定目录服务器操作的索引类型，并取要索引的属性值。每个所需的索引类型都必须在单独的行中输入。

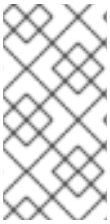
参数	描述
条目 DN	cn=default indexes,cn=config,cn=ldbm database,cn=plugins,cn=config
有效值	* pres = presence index * EQ = 相等索引 * approx = 大约索引 * sub = 子字符串索引 * 匹配规则 = 国际索引 * index browse = 浏览索引
默认值	
语法	DirectoryString
示例	nsIndexType: eq

6.4.8.4. nsMatchingRule

此可选的多值属性指定匹配规则名称或 OID 的排序，用于匹配值并为属性生成索引键。这最常用于确保相等和范围搜索可针对英语以外的语言(7-bit ASCII)正常工作。

这还用于允许范围搜索在架构定义中指定排序匹配规则的整数语法属性。uidNumber 和 gidNumber 是两个常用的属性，它们属于此类别。

例如，对于使用整数语法的 uidNumber，rule 属性可以是 nsMatchingRule: integerOrderingMatch。



注意

对此属性的任何更改都不会生效，直到保存更改并且使用 db2index 命令重新构建索引。

参数	描述
条目 DN	cn=default indexes,cn=config,cn=ldbm database,cn=plugins,cn=config
有效值	任何有效的 collation order 对象标识符(OID)
默认值	无
语法	DirectoryString
示例	nsMatchingRule: 2.16.840.1.113730.3.3.2.3.1 （对于 Bulgarian）

6.4.8.5. nsSystemIndex

此强制属性指定索引是否为 系统索引，这是目录服务器操作至关重要的索引。如果此属性的值为 true，则它是 system-essential。系统索引不应被删除，因为这会严重破坏服务器功能。

参数	描述
条目 DN	cn=default indexes,cn=config,cn=ldbm database,cn=plugins,cn=config
有效值	true | false
默认值	
语法	DirectoryString
示例	nssystemindex: true

6.4.9. cn=index,cn=database_name,cn=ldbm database,cn=plugins,cn=config 下的数据库属性

除了在 cn=default 索引下存储的默认 索引集，cn=config,cn=ldbm database,cn=plugins,cn=config，可以为用户定义的后端实例创建自定义索引；它们存储在 cn=index,cn=database_name,cn=ldbm database,cn=plugins,cn=config 下。

例如，o=UserRoot 下的 aci 属性的索引文件会出现在 Directory Server 中，如下所示：

```
dn:cn=aci,cn=index,cn=UserRoot,cn=ldbm database,cn=plugins,cn=config
objectclass:top
objectclass:nsIndex
cn:aci
nsSystemIndex:true
nsIndexType:pres
```

这些条目共享为 第 6.4.8 节 “cn=default index,cn=config,cn=ldbm database,cn=plugins,cn=config 下的数据库属性” 中的默认索引列出的所有索引属性。

6.4.9.1. nsIndexIDListScanLimit

此多值参数定义特定索引的搜索限制，或不使用 ID 列表。

参数	描述
条目 DN	cn=*attribute_name*,cn=index,cn=*database_name*,cn=ldbm database,cn=plugins,cn=config
有效值	
默认值	
语法	DirectoryString
示例	nsIndexIDListScanLimit: limit=0 type=eq values=inetorgperson

6.4.9.2. nsSubStrBegin

默认情况下，要索引搜索，搜索字符串必须至少为三个字符，而不计算任何通配符字符。例如，字符串 abc 将是一个索引搜索，而 ab* 则不行。索引的搜索比未索引搜索要快，因此更改搜索键的最小长度有助于增加索引搜索的数量。

这个子字符串长度可以根据任何通配符字符的位置编辑。nsSubStrBegin 属性在通配符前面为搜索字符串的开头设置索引搜索所需的字符数。例如：

```
abc*
```

如果更改了此属性的值，则必须使用 db2index 重新生成索引。

参数	描述
条目 DN	cn=*attribute_name*,cn=index,cn=*database_name*,cn=ldbm database,cn=plugins,cn=config
有效值	任何整数
默认值	3
语法	整数
示例	nsSubStrBegin: 2

6.4.9.3. nsSubStrEnd

默认情况下，要索引搜索，搜索字符串必须至少为三个字符，而不计算任何通配符字符。例如，字符串 abc 将是一个索引搜索，而 ab 则不行。索引的搜索比未索引搜索要快，因此更改搜索键的最小长度有助于增加索引搜索的数量。*

这个子字符串长度可以根据任何通配符字符的位置编辑。nsSubStrEnd 属性在通配符后为搜索字符串末尾设置索引搜索所需的字符数。例如：

```
*xyz
```

如果更改了此属性的值，则必须使用 db2index 重新生成索引。

参数	描述
条目 DN	cn=*attribute_name*,cn=index,cn=*database_name*,cn=ldbm database,cn=plugins,cn=config
有效值	任何整数
默认值	3
语法	整数
示例	nsSubStrEnd: 2

6.4.9.4. nsSubStrMiddle

默认情况下，要索引搜索，搜索字符串必须至少为三个字符，而不计算任何通配符字符。例如，字符串 abc 将是一个索引搜索，而 ab* 则不行。索引的搜索比未索引搜索要快，因此更改搜索键的最小长度有助于增加索引搜索的数量。

这个子字符串长度可以根据任何通配符字符的位置编辑。nsSubStrMiddle 属性为索引搜索设置所需的字符数，其中搜索字符串中间使用通配符。例如：

```
ab*z
```

如果更改了此属性的值，则必须使用 db2index 重新生成索引。

参数	描述
条目 DN	cn=*attribute_name*,cn=index,cn=*database_name*,cn=ldbm database,cn=plugins,cn=config
有效值	任何整数
默认值	3
语法	整数
示例	nsSubStrMiddle: 3

6.4.10. cn=attribute_name,cn=encrypted attributes,cn=database_name,cn=ldbm database,cn=plugins,cn=config 下的数据库属性

除了在 cn=default 索引下存储的默认 索引集，cn=config,cn=ldbm database,cn=plugins,cn=config，可以为用户定义的后端实例创建自定义索引；它们存储在 cn=index,cn=database_name,cn=ldbm database,cn=plugins,cn=config 下。

例如，o=UserRoot 下的 aci 属性的索引文件会出现在 Directory Server 中，如下所示：

```
dn:cn=aci,cn=index,cn=UserRoot,cn=ldbm database,cn=plugins,cn=config
objectclass:top
objectclass:nsIndex
cn:aci
nsSystemIndex:true
nsIndexType:pres
```

这些条目共享为 第 6.4.8 节 “cn=default index,cn=config,cn=ldbm database,cn=plugins,cn=config 下的数据库属性” 中的默认索引列出的所有索引属性。

6.4.10.1. nsIndexIDListScanLimit

此多值参数定义特定索引的搜索限制，或不使用 ID 列表。

参数	描述
条目 DN	cn=*attribute_name*,cn=index,cn=*database_name*,cn=ldbm database,cn=plugins,cn=config
有效值	
默认值	
语法	DirectoryString
示例	nsIndexIDListScanLimit: limit=0 type=eq values=inetorgperson

6.4.10.2. nsSubStrBegin

默认情况下，要索引搜索，搜索字符串必须至少为三个字符，而不计算任何通配符字符。例如，字符串 abc 将是一个索引搜索，而 ab* 则不行。索引的搜索比未索引搜索要快，因此更改搜索键的最小长度有助于增加索引搜索的数量。

这个子字符串长度可以根据任何通配符字符的位置编辑。nsSubStrBegin 属性在通配符前面为搜索字符串的开头设置索引搜索所需的字符数。例如：

```
abc*
```

如果更改了此属性的值，则必须使用 db2index 重新生成索引。

参数	描述
条目 DN	cn=*attribute_name*,cn=index,cn=*database_name*,cn=ldbm database,cn=plugins,cn=config
有效值	任何整数

参数	描述
默认值	3
语法	整数
示例	nsSubStrBegin: 2

6.4.10.3. nsSubStrEnd

默认情况下，要索引搜索，搜索字符串必须至少为三个字符，而不计算任何通配符字符。例如，字符串 abc 将是一个索引搜索，而 ab* 则不行。索引的搜索比未索引搜索要快，因此更改搜索键的最小长度有助于增加索引搜索的数量。

这个子字符串长度可以根据任何通配符字符的位置编辑。nsSubStrEnd 属性在通配符后为搜索字符串末尾设置索引搜索所需的字符数。例如：

```
*xyz
```

如果更改了此属性的值，则必须使用 db2index 重新生成索引。

参数	描述
条目 DN	cn=*attribute_name*,cn=index,cn=*database_name*,cn=ldbm database,cn=plugins,cn=config
有效值	任何整数
默认值	3
语法	整数
示例	nsSubStrEnd: 2

6.4.10.4. nsSubStrMiddle

默认情况下，要索引搜索，搜索字符串必须至少为三个字符，而不计算任何通配符字符。例如，字符串 abc 将是一个索引搜索，而 ab* 则不行。索引的搜索比未索引搜索要快，因此更改搜索键的最小长度有助于增加索引搜索的数量。

这个子字符串长度可以根据任何通配符字符的位置编辑。nsSubStrMiddle 属性为索引搜索设置所需

的字符数，其中搜索字符串中间使用通配符。例如：

> *ab*z*

如果更改了此属性的值，则必须使用 db2index 重新生成索引。

参数	描述
条目 DN	cn=*attribute_name*,cn=index,cn=*database_name*,cn=ldbm database,cn=plugins,cn=config
有效值	任何整数
默认值	3
语法	整数
示例	nsSubStrMiddle: 3

6.5. 数据库链接插件属性

数据库链接插件属性也以信息树中组织。数据库链接实例使用的所有插件技术都存储在 cn=chaining 数据库 插件节点中。本节显示了在图中的 cn=chaining database,cn=plugins,cn=config 信息树中标为粗体的三个节点的额外属性信息。

6.5.1. cn=config,cn=chaining database,cn=plugins,cn=config 下的数据库链接属性

本节涵盖所有实例通用的全局配置属性，存储在 cn=config,cn=chaining database,cn=plugins,cn=config 树中。

6.5.1.1. nsActiveChainingComponents

此属性使用链列出组件。组件是服务器中的任何功能单元。此属性的值覆盖全局配置属性中的值。要禁用特定数据库实例上的链，请使用值 None。此属性还允许更改用于链的组件。默认情况下，不允许组件链，它解释了为什么此属性可能无法出现在 cn=config,cn=chaining database,cn=config 属性列表中，因为 LDAP 认为空属性不存在。

参数	描述

参数	描述
条目 DN	cn=config,cn=chaining database,cn=plugins,cn=config
有效值	任何有效的组件条目
默认值	无
语法	DirectoryString
示例	nsActiveChainingComponents: cn=uid uniqueness,cn=plugins,cn=config

6.5.1.2. nsMaxResponseDelay

此错误检测，与性能相关的属性指定在怀疑错误之前，远程服务器可以对数据库链接发出的 LDAP 操作请求的最大时间。满足此延迟周期后，数据库链接会测试与远程服务器的连接。

参数	描述
条目 DN	cn=config,cn=chaining database,cn=plugins,cn=config
有效值	任何有效的延迟周期（以秒为单位）
默认值	60 秒
语法	整数
示例	nsMaxResponseDelay: 60

6.5.1.3. nsMaxTestResponseDelay

此错误检测，与性能相关的属性指定数据库链接发布的测试持续时间，以检查远程服务器是否响应。如果在通过此周期之前没有返回来自远程服务器的响应，数据库链接会假定远程服务器停机，且连接不会用于后续操作。

参数	描述
条目 DN	cn=config,cn=chaining database,cn=plugins,cn=config

参数	描述
有效值	任何有效的延迟周期（以秒为单位）
默认值	15 秒
语法	整数
示例	nsMaxTestResponseDelay: 15

6.5.1.4. nsTransmittedControls

此属性可以是全局（以及动态）配置或实例（即 cn=database link instance,cn=chaining database,cn=plugins,cn=config）配置属性，允许控制数据库链接转发。默认情况下，数据库链接会转发以下控制：

- ***受管 DSA (OID: 2.16.840.1.113730.3.4.2)***
- ***虚拟列表视图(VLV) (OID: 2.16.840.1.113730.3.4.9)***
- ***服务器端排序(OID: 1.2.840.113556.1.4.473)***
- ***循环检测(OID: 1.3.6.1.4.1.1466.29539.12)***

其他控制，如取消引用和简单页面搜索的结果，可以添加到要转发的控制列表中。

参数	描述
条目 DN	cn=config,cn=chaining database,cn=plugins,cn=config
有效值	由数据库链接转发的任何有效的 OID 或以上列出的控制
默认值	无
语法	整数

参数	描述
示例	nsTransmittedControls: 1.2.840.113556.1.4.473

6.5.2. cn=default 实例 config,cn=chaining database,cn=plugins,cn=config 下的数据库链接属性

实例的默认实例配置属性存储在 cn=default 实例配置,cn=chaining database,cn=plugins,cn=config 树中。

6.5.2.1. nsAbandonedSearchCheckInterval

此属性显示服务器检查带操作前传递的秒数。

参数	描述
条目 DN	cn=default 实例 config,cn=chaining database,cn=plugins,cn=config
有效范围	0 到最大 32 位整数(2147483647)
默认值	1
语法	整数
示例	nsAbandonedSearchCheckInterval: 10

6.5.2.2. nsBindConnectionsLimit

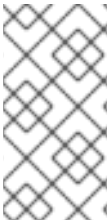
此属性显示数据库链路与远程服务器建立的最大 TCP 连接数。

参数	描述
条目 DN	cn=default 实例 config,cn=chaining database,cn=plugins,cn=config
有效范围	1 到 50 个连接
默认值	3
语法	整数

参数	描述
示例	nsBindConnectionsLimit: 3

6.5.2.3. nsBindRetryLimit

与名称的建议不同，此属性没有指定数据库链接重新尝试与远程服务器绑定的次数。此处的值 1 表示数据库链接只尝试绑定一次。



注意

重试只在连接失败时发生，而不适用于其他类型的错误，如无效的绑定 DN 或错误的密码。

参数	描述
条目 DN	cn=default 实例 config,cn=chaining database,cn=plugins,cn=config
有效范围	0 到 5
默认值	3
语法	整数
示例	nsBindRetryLimit: 3

6.5.2.4. nsBindTimeout

此属性显示绑定尝试超时前的时间长度。这个属性没有实际有效的范围，但合理的时钟限制除外。

参数	描述
条目 DN	cn=default 实例 config,cn=chaining database,cn=plugins,cn=config
有效范围	0 到 60 秒
默认值	15
语法	整数

参数	描述
示例	nsBindTimeout: 15

6.5.2.5. nsCheckLocalACI

仅用于高级使用。此属性控制 ACI 是否在数据库链接和远程数据服务器上评估。对此属性的更改仅在服务器重启后生效。

参数	描述
条目 DN	cn=default 实例 config,cn=chaining database,cn=plugins,cn=config
有效值	on | off
默认值	off
语法	DirectoryString
示例	nsCheckLocalACI: on

6.5.2.6. nsConcurrentBindLimit

此属性显示每个 TCP 连接的最大并发绑定操作数。

参数	描述
条目 DN	cn=default 实例 config,cn=chaining database,cn=plugins,cn=config
有效范围	1 到 25 个绑定
默认值	10
语法	整数
示例	nsConcurrentBindLimit: 10

6.5.2.7. nsConcurrentOperationsLimit

此属性指定允许的最大并发操作数。

参数	描述
条目 DN	cn=default 实例 config,cn=chaining database,cn=plugins,cn=config
有效范围	1 到 50 个操作
默认值	2
语法	整数
示例	nsConcurrentOperationsLimit: 5

6.5.2.8. nsConnectionLife

此属性指定连接生命周期。在特定时间段内，数据库链接和远程服务器之间的连接可以保持打开。连接保持打开速度更快，但它使用更多资源。当值为 0 且在 nsFarmServerURL 属性中提供故障转移服务器列表时，主服务器在故障转移到备用服务器后永远不会联系。

参数	描述
条目 DN	cn=default 实例 config,cn=chaining database,cn=plugins,cn=config
有效范围	0 代表无限秒数（其中 0 表示永久）
默认值	0
语法	整数
示例	nsConnectionLife: 0

6.5.2.9. nsOperationConnectionsLimit

此属性显示数据库链路与远程服务器建立的最大 LDAP 连接数。

参数	描述

参数	描述
条目 DN	cn=default 实例 config,cn=chaining database,cn=plugins,cn=config
有效范围	1 到 n 连接
默认值	20
语法	整数
示例	nsOperationConnectionsLimit: 10

6.5.2.10. nsProxiedAuthorization

仅用于高级使用。如果您禁用代理授权，则链操作的绑定作为 nsMultiplexorBindDn 属性中设置的用户执行。

参数	描述
条目 DN	cn=default 实例 config,cn=chaining database,cn=plugins,cn=config
有效值	on | off
默认值	on
语法	DirectoryString
示例	nsProxiedAuthorization: on

6.5.2.11. nsReferralOnScopedSearch

此属性控制是否通过范围搜索返回引用。此属性可用于优化目录，因为返回引用以响应有范围搜索更为高效。返回所有配置的场服务器。

参数	描述
条目 DN	cn=default 实例 config,cn=chaining database,cn=plugins,cn=config
有效值	on | off

参数	描述
默认值	off
语法	DirectoryString
示例	nsReferralOnScopedSearch: off

6.5.2.12. nsSizeLimit

此属性以字节为单位显示数据库链接的默认大小限制。

参数	描述
条目 DN	cn=default 实例 config,cn=chaining database,cn=plugins,cn=config
有效范围	-1（无限制）最多 32 位整数(2147483647)条目
默认值	2000
语法	整数
示例	nsSizeLimit: 2000

6.5.2.13. nsTimeLimit

此属性显示数据库链接的默认搜索时间限制。

参数	描述
条目 DN	cn=default 实例 config,cn=chaining database,cn=plugins,cn=config
有效范围	-1 到最大 32 位整数(2147483647)
默认值	3600
语法	整数
示例	nsTimeLimit: 3600

6.5.3. cn=database_link_name,cn=chaining database,cn=plugins,cn=config 下的数据库链接属性

此信息节点存储与包含数据的服务器相关的属性。场服务器 是包含数据库数据的服务器。此属性可以包含用于故障转移的可选服务器，用空格分开。对于级联链，此 URL 可以指向另一个数据库链接。

6.5.3.1. nsBindMechanism

此属性设置用于连接到远程服务器的场服务器绑定机制。场服务器是包含一个或多个数据库中数据的服务器。此属性配置连接类型，可以是 standard、TLS 或 SASL。

- 空。这会执行简单的身份验证，并且需要 nsMultiplexorBindDn 和 nsMultiplexorCredentials 属性来提供绑定信息。
- 外部.这使用 TLS 证书向远程服务器验证场服务器。场服务器 URL 必须设置为安全 URL (ldaps)，或者 nsUseStartTLS 属性必须设置为 上的。

  此外，必须将远程服务器配置为将 farm 服务器证书映射到其绑定身份。
- DIGEST-MD5.这使用带有 DIGEST-MD5 加密的 SASL。与简单的身份验证一样，这需要 nsMultiplexorBindDn 和 nsMultiplexorCredentials 属性提供绑定信息。
- GSSAPI。这通过 SASL 使用基于 Kerberos 的身份验证。场服务器必须通过标准端口连接，这意味着 URL 具有 ldap，因为目录服务器不支持 TLS 的 SASL/GS-API。

  场服务器必须配置 Kerberos keytab，远程服务器必须具有场服务器绑定身份的定义的 SASL 映射。

参数	描述
条目 DN	cn=*database_link_name*,cn=chaining database,cn=plugins,cn=config
有效值	* 空 * 外部 * DIGEST-MD5 * GSSAPI

参数	描述
默认值	empty
语法	DirectoryString
示例	nsBindMechanism: GSSAPI

6.5.3.2. nsFarmServerURL

此属性提供远程服务器的 LDAP URL。场服务器是包含一个或多个数据库中数据的服务器。此属性可以包含用于故障转移的可选服务器，用空格分开。如果使用级联更改，此 URL 可以指向另一个数据库链接。

参数	描述
条目 DN	cn=*database_link_name*,cn=chaining database,cn=plugins,cn=config
有效值	任何有效的远程服务器 LDAP URL
默认值	
语法	DirectoryString
示例	nsFarmServerURL: ldap://farm1.example.com farm2.example.com:389 farm3.example.com:1389/

6.5.3.3. nshoplimit

此属性指定允许数据库链的最大次数；即，请求可以从一个数据库链接转发到另一个数据库的次数。

参数	描述
条目 DN	cn=*database_link_name*,cn=chaining database,cn=plugins,cn=config
有效范围	1 到适合部署的上限
默认值	10
语法	整数

参数	描述
示例	nsHopLimit: 3

6.5.3.4. nsMultiplexorBindDN

此属性提供用于与远程服务器通信的管理条目的 DN。multiplexor 是包含数据库链接并与场服务器进行通信的服务器。此绑定 DN 不能是 Directory Manager，如果没有指定此属性，数据库链接绑定为 匿名。

参数	描述
条目 DN	cn=*database_link_name*,cn=chaining database,cn=plugins,cn=config
有效值	
默认值	多路的 DN
语法	DirectoryString
示例	nsMultiplexerBindDN: cn=proxy manager

6.5.3.5. nsMultiplexorCredentials

管理用户的密码，以纯文本形式提供。如果没有提供密码，这表示用户可以绑定为 匿名。密码在配置文件中加密。下面的示例显示什么，而不是键入的内容。

参数	描述
条目 DN	cn=*database_link_name*,cn=chaining database,cn=plugins,cn=config
有效值	任何有效的密码，然后使用 DES 反向密码加密模式对其进行加密
默认值	
语法	DirectoryString
示例	nsMultiplexerCredentials: {DES} 9Eko69APCJfF

6.5.3.6. nsUseStartTLS

此属性设定是否使用 Start TLS 通过不安全的端口启动安全加密的连接。如果 nsBindMechanism 属性设置为 EXTERNAL，但 farm 服务器 URL 设置为标准 URL (ldap)，或者 nsBindMechanism 属性为空，则可以使用此属性。

参数	描述
条目 DN	cn=*database_link_name*,cn=chaining database,cn=plugins,cn=config
有效值	off | on
默认值	off
语法	DirectoryString
示例	nsUseStartTLS: on

6.5.4. cn=monitoring,cn=database_link_name,cn=chaining database,cn=plugins,cn=config 下的数据库链接属性

用于监控实例上的活动的属性存储在 cn=monitor,cn=database instance name,cn=chaining database,cn=plugins,cn=config 信息树中。

6.5.4.1. nsAbandonCount

此属性提供收到的带外操作数量。

6.5.4.2. nsAddCount

此属性提供收到的 add 操作数量。

6.5.4.3. nsBindCount

此属性提供收到的绑定请求数。

6.5.4.4. nsCompareCount

此属性提供收到的比较操作数量。

6.5.4.5. nsDeleteCount

此属性提供收到的 delete 操作数量。

6.5.4.6. nsModifyCount

此属性提供收到的修改操作数量。

6.5.4.7. nsOpenBindConnectionCount

此属性提供绑定操作的打开连接数量。

6.5.4.8. nsOperationConnectionCount

此属性提供正常操作的打开连接数量。

6.5.4.9. nsRenameCount

此属性提供收到的重命名操作数量。

6.5.4.10. nsSearchBaseCount

此属性提供收到的基本级别搜索数量。

6.5.4.11. nsSearchOneLevelCount

此属性提供收到的单级搜索数量。

6.5.4.12. nsSearchSubtreeCount

此属性提供收到的子树搜索数量。

6.5.4.13. nsUnbindCount

此属性提供收到的未绑定数量。

6.6. 引用完整性插件属性

参考完整性可确保当您对目录中条目执行更新或删除操作时，服务器还会更新引用已删除/更新的条目的信息。例如，如果从目录中删除了用户条目并启用了引用完整性，服务器也会从用户所属的任何组中删除该用户。

6.6.1. nsslapd-pluginAllowReplUpdates

参考完整性可能是一个非常资源要求的过程。因此，如果您配置了多层次复制，则引用完整性插件将默认忽略复制更新。但是，有时无法启用引用完整性插件，或者插件不可用。

例如，复制拓扑中的其中一个供应商是 Active Directory （更多详情请参阅 Windows 同步 章节），它们不支持引用完整性。在这种情况下，您可以允许其他供应商上的 referential Integrity 插件使用 nsslapd-pluginAllowReplUpdates 属性处理复制更新。

重要

在 multi-supplier 复制拓扑中，只有一个供应商必须具有 nsslapd-pluginAllowReplUpdates 属性值。否则，可能会导致复制错误，并需要完全初始化来修复问题。另一方面，在可能的情况下，所有提供都必须启用 referential Integrity 插件。

参数	描述
条目 DN	cn=referential integrity postoperation,cn=plugins,cn=config
有效范围	on/off
默认值	off
语法	布尔值
示例	nsslapd-pluginAllowReplUpdates: off

第 7 章 模式定义

目录架构是一组定义如何在目录中存储数据的规则。目录信息存储离散条目，每个条目由一组属性及其值组成。条目中描述的身份类型在条目的对象类中定义。对象类指定条目通过对象类定义的一组属性描述的对象类型。

基本上，架构文件是可以创建(对象类)以及这些条目可以描述(属性)的条目类型的列表。架构 定义 对象类和属性是什么。架构还定义了属性值包含的格式（属性 的语法），以及是否只能是该属性的单一实例。

可以将其他架构文件添加到目录服务器配置中并加载到服务器中，因此可以自定义该架构，并可根据需要进行扩展。

警告

如果模式定义包含太多字符，目录服务器无法启动。在那些中，LDAP 标准允许使用零个或多个空格；例如，NAME 关键字与属性类型名称之间的位置。

7.1. 对象类

在 LDAP 中，对象类定义可用于定义条目的属性集合。LDAP 标准为许多常用条目提供对象类，如人员和 inetOrgPerson）、组(groupOfUniqueNames)、位置(locality)、机构和部门(机构 和 机构单元)和设备(设备)。

在架构文件中，对象类由 objectclasses 行标识，然后是其 OID、名称、描述、其直接的对象类（需要与对象类一同使用的对象类，并与这个对象类共享其属性）以及所需的(MUST)和允许(MAY)属性的列表。以下示例中显示了：

例 7.1. 人员对象类架构条目

```
objectClasses: ( 2.5.6.6 NAME 'person' DESC 'Standard LDAP objectclass' SUP top MUST ( sn $ cn ) MAY ( description $ seeAlso $ telephoneNumber $ userPassword ) X-ORIGIN 'RFC 2256' )
```

7.1.1. 必要和允许的属性

每个对象类定义了多个所需属性和允许的属性。所需属性必须使用指定的对象类存在于条目中，而允许的属性会被禁止使用且可用于条目，但该条目不需要有效。

与 例 7.1 “人员对象类架构条目” 中一样，person 对象类需要 cn,sn, 和 iwl 属性，并允许 描述,seeAlso,telephoneNumber, 和 userPassword 属性。

注意

所有条目都需要 zFCP 属性，它列出了分配给该条目的对象类。

7.1.2. 对象类继承

个条目可以有多个对象类。例如，个人对象类条目由 person 对象类定义，但同一人也可能由 inetOrgPerson 和 organizationalPerson 对象类中的属性描述。

此外，对象类可以是分级。除了自己的必需和允许的属性外，对象类也可以从另一个类继承属性。第二个对象类是第一个 顶级 的对象类。

服务器的对象类结构决定了特定条目所需和允许的属性列表。例如，用户条目必须具有 inetOrgPerson 对象类。在这种情况下，该条目还必须包括 inetOrgPerson,organizationalPerson, 和 organizationalPerson 的 superior 对象类，即 organizationalPerson 的高级对象类，即：

```
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
```

当将 inetOrgPerson 对象类分配给条目时，该条目会自动继承来自高级对象类的必需属性和允许的属性。

7.2. 属性

目录条目由属性及其值组成。这些对称为 属性-值断言 或 AVAs。目录中的任何信息都与描述性属性关联。例如，cn 属性用于存储个人的完整名称，如 cn: John Smith。

其他属性可以提供有关 John Smith 的更多信息：

```
givenname: John
surname: Smith
mail: jsmith@example.com
```

在架构文件中，属性由 attributetypes 行标识，后跟其 OID, name, description, description, syntax, syntax (allowed format for its value), attribute is single- or multi-valued，以及属性的定义位置。

以下示例中显示了：

例 7.2. 描述属性架构条目

```
attributetypes: ( 2.5.4.13 NAME 'description' DESC 'Standard LDAP attribute type' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 X-ORIGIN 'RFC 2256' )
```

某些属性可以缩写。这些缩写列为属性定义的一部分：

```
attributetypes: ( 2.5.4.3 NAME ( 'cn' 'commonName' ) ...
```

7.2.1. 目录服务器属性语法

属性的语法定义了属性允许的值的格式；与其他架构元素一样，使用 schema 文件条目中语法的 OID 为属性定义语法。

目录服务器使用属性的语法对条目执行排序和模式匹配。

有关 LDAP 属性语法的更多信息，请参阅 RFC 4517。

表 7.1. 支持的 LDAP 属性语法

名称	OID	定义
二进制	1.3.6.1.4.1.1466.115.121.1.5	已弃用。改为使用 Octet 字符串。
位字符串	1.3.6.1.4.1.1466.115.121.1.6	对于值为位的值，如 **'0101111101'B**。
布尔值	1.3.6.1.4.1.1466.115.121.1.7	对于只有两个允许的值的属性，TRUE 或 FALSE。

名称	OID	定义
国家/地区字符串	1.3.6.1.4.1.1466.115.121.1.11	对于限制为正好两个可打印的字符串字符的值；例如，US 代表美国。
DN	1.3.6.1.4.1.1466.115.121.1.12	对于可区分名称(DN)的值。
交付方法	1.3.6.1.4.1.1466.115.121.1.14	对于包含提供信息或联系实体的首选方法的值。不同的值使用美元符号($)分隔。例如： [literal,subs="+quotes",options="nowrap",role=white-space-pre] .... telephone $ physical ....
目录字符串	1.3.6.1.4.1.1466.115.121.1.15	对于有效 UTF-8 字符串的值。这些值不一定区分大小写。区分大小写和不区分大小写的匹配规则都可用于目录字符串和相关语法。
增强的指南	1.3.6.1.4.1.1466.115.121.1.21	对于包含基于属性和过滤器的复杂搜索参数的值。
Facsimile	1.3.6.1.4.1.1466.115.121.1.22	包含 fax 号的值。
传真	1.3.6.1.4.1.1466.115.121.1.23	包含传输传真的镜像的值。
常规时间	1.3.6.1.4.1.1466.115.121.1.24	对于编码为可打印字符串的值。必须指定时区。强烈建议您使用 GMT 时间。
指南	1.3.6.1.4.1.1466.115.121.1.25	*过时。*对于包含基于属性和过滤器的复杂搜索参数的值。
IA5 字符串	1.3.6.1.4.1.1466.115.121.1.26	作为有效字符串的值。这些值不一定区分大小写。IA5 字符串和相关语法都提供了区分大小写且不区分大小写的匹配规则。
整数	1.3.6.1.4.1.1466.115.121.1.27	对于整个数字的值。
JPEG	1.3.6.1.4.1.1466.115.121.1.28	包含镜像数据的值。
名称和可选 UID	1.3.6.1.4.1.1466.115.121.1.34	对于包含 DN 和（可选）唯一 ID 的组合值的值。
数字字符串	1.3.6.1.4.1.1466.115.121.1.36	对于包含 numerals 和空格的字符串的值。

名称	OID	定义
OctetString	1.3.6.1.4.1.1466.115.121.1.40	对于二进制值；这将替换二进制语法。
对象类描述	1.3.6.1.4.1.1466.115.121.1.37	包含对象类定义的值。
OID	1.3.6.1.4.1.1466.115.121.1.38	包含 OID 定义的值。
邮政地址	1.3.6.1.4.1.1466.115.121.1.41	对于采用 **postal-address =** *dstring* ***("$"** *dstring***)** 格式编码的值。例如： [literal,subs="+quotes",options="nowrap",role=white-space-pre] ... .1234 主 St.$Raleigh, NC 12345$USA .... 每个 *dstring* 组件都编码为 DirectoryString 值。如果发生反斜杠和美元字符，则用引号括起来，因此不会对行分隔符出错。许多服务器将邮政地址限制为最多 30 个字符的 6 行。
可打印的字符串	1.3.6.1.4.1.1466.115.121.1.44	包含可打印字符串的值。
space-Insensitive String	2.16.840.1.113730.3.7.1	包含空格敏感字符串的值。
telephoneNumber	1.3.6.1.4.1.1466.115.121.1.50	对于以电话号码形式的值。建议您使用国际格式的电话号码。
Teletex Terminal Identifier	1.3.6.1.4.1.1466.115.121.1.51	包含国际电话号码的值。
Telex Number	1.3.6.1.4.1.1466.115.121.1.52	对于包含电话号、国家代码和电话终端的回答代码的值。
URI		对于 URL 形式的值，如 **http://**、**https://**、**ftp://**、**ldap://** 和 **ldaps://** 等字符串。URI 与 IA5 字符串具有相同的行为。有关此语法的更多信息，请参阅 RFC 4517。

7.2.2. 单值和多值属性

默认情况下，大多数属性都是多值。这意味着条目可以多次包含同一属性，其值不同。例如：

```
dn: uid=jsmith,ou=marketing,ou=people,dc=example,dc=com
ou: marketing
ou: people
```

例如，cn、tel 和 objectclass 属性都有多个值。单值的属性 - 也就是说，只能指定属性的一个实例 - 在 schema 中指定，只允许单个值。例如，uidNumber 只能有一个可能的值，因此其 schema 条目具有术语 SINGLE-VALUE。如果属性是多值，则没有值 expression。

7.3. 默认目录服务器模式文件

目录服务器的模板 schema 定义存储在 /etc/dirsrv/schema 目录中。这些默认模式文件用于生成新目录服务器实例的模式文件。每个服务器实例在 /etc/dirsrv/slapd-instance/schema 中都有自己的特定于实例的模式目录。实例目录中的架构文件仅供该实例使用。

要修改目录架构，请在特定于实例的 schema 目录中创建新的属性和新对象类。由于默认架构用于创建新实例，并且每个实例都有自己的架构文件，因此每个实例可能会略有不同模式，与每个实例的使用相匹配。

使用 LDAP 命令添加的任何自定义属性都存储在 99user.ldif 文件中；其他自定义模式文件可以添加到每个实例的 /etc/dirsrv/slapd-instance/schema 目录中。不要对 {PRODUCT} 附带的标准文件进行任何修改。

表 7.2. 模式文件

模式文件	用途
00core.ldif	X.500 和 LDAP 标准(RFC)的建议内核模式。此模式供目录服务器本身用于实例配置并启动服务器实例。
01core389.ldif	X.500 和 LDAP 标准(RFC)的建议内核模式。此模式供目录服务器本身用于实例配置并启动服务器实例。
02common.ldif	来自 RFC 2256、LDAPv3 和标准模式的标准架构，用来配置条目。
05rfc2927.ldif	来自 RFC 2927 的 schema，"MIME Directory Profile for LDAP Schema"。
05rfc4523.ldif	X.509 证书的 schema 定义。
05rfc4524.ldif	Cosine LDAP/X.500 模式。
06inetorgperson.ldif	来自 RFC 2798、RFC 2079 和 RFC 1274 的 inetOrgPerson 模式元素。

模式文件	用途
10rfc2307.ldif	RFC 2307，"将 LDAP 用作网络信息服务的方法"。
20subscriber.ldif	Directory Server-Nortel 订阅者互操作性的常见 schema 元素。
25java-object.ldif	RFC 2713 中的模式，"用于代表 LDAP 目录中的 Java 对象的架构"。
28pilot.ldif	试用 RFC （特别是 RFC 1274）中的模式，在新部署中不再推荐使用。
30ns-common.ldif	常见模式.
50ns-admin.ldif	管理服务器使用的模式。
50ns-certificate.ldif	Red Hat Certificate System 使用的模式。
50ns-directory.ldif	传统目录服务器 4.x 服务器使用的 schema。
50ns-mail.ldif	邮件服务器的 schema。
50ns-value.ldif	用于 Directory Server 中值项的 schema。
50ns-web.ldif	Web 服务器的 schema。
60autofs.ldif	用于自动挂载配置的对象类 ; 这是用于 NIS 服务器的多种架构文件之一。
60eduperson.ldif	教育相关人员和组织条目的模式元素。
60mozilla.ldif	Mozilla 相关用户配置文件的 schema 元素。
60nss-ldap.ldif	GSS-API 服务名称的架构元素。
60pam-plugin.ldif	用于将目录服务与 PAM 模块集成的 schema 元素。
60pureftpd.ldif	用于定义 FTP 用户帐户的模式元素。
60rfc2739.ldif	日历和 vCard 属性的 schema 元素。
60rfc3712.ldif	用于配置打印机的 schema 元素。
60sabayon.ldif	用于定义 sabayon 用户条目的 schema 元素。
60sudo.ldif	用于定义 sudo 用户和角色的 schema 元素。

模式文件	用途
60trust.ldif	用于定义 NSS 或 PAM 的信任关系的 schema 元素。
99user.ldif	自定义架构元素

7.4. 对象标识符

所有架构元素都分配有对象标识符(OID)，包括属性和对象类。OID 是整数的序列，通常写为点分隔的字符串。所有自定义属性和类都必须符合 X.500 和 LDAP 标准。

警告

如果没有为 schema 元素指定 OID，Directory 服务器会自动使用 ObjectClass_name-oid 和 attribute_name-oid。但是，强烈建议使用文本 OID 而不是数字 OID 会导致客户端、服务器互操作性和服务器行为出现问题。

OID 可以基于.基本 OID 是一个根号，用于一个机构的每个 schema 元素，然后可以递增 schema 元素。例如，基础 OID 可以是 1。然后，公司将 1.1 用于属性，因此每个新属性的 OID 为 1.1.x。它对对象类使用 1.2，因此每个新对象类都有一个 OID 为 1.2.x。

对于 Directory Server 定义的 schema 元素，基础 OID 如下：

- Netscape 基础 OID 为 2.16.840.1.113730。
- 目录服务器基础 OID 是 2.16.840.1.113730.3。
- 所有 Netscape-defined 属性都具有基础 OID 2.16.840.1.113370.3.1。
- 所有 Netscape 定义的对象类都有 base OID 2.16.840.1.113730.3.2。

有关 OID 或请求前缀的更多信息，请访问互联网编号分配机构(IANA)网站，网址为 http://www.iana.org/。

7.5. 扩展架构

目录服务器架构包含数百个对象类和属性，可用于满足大多数目录要求。此模式可以使用新的对象类和属性进行扩展，它们通过创建自定义架构文件来满足企业中目录服务的演进要求。

在向架构添加新属性时，应创建一个新的对象类来包含它们。在现有对象类中添加新属性可能会破坏目录服务器与依赖标准 LDAP 模式的现有 LDAP 客户端的兼容性，并可能会在升级服务器时造成困难。

7.6. 模式检查

架构检查 意味着目录服务器会在创建、修改或使用 LDIF 导入的数据库时检查每个条目，以确保它符合 schema 文件中的模式定义。架构检查会验证以下三个操作：

- 条目中使用的对象类和属性在目录 schema 中定义。
- 对象类所需的属性包含在条目中。
- 只有对象类允许的属性包含在条目中。

您应该在打开模式检查的情况下运行目录服务器。

7.7. 语法验证

语法验证 意味着目录服务器检查属性值是否与该属性所需的语法匹配。例如，语法验证将确认一个新的 telephoneNumber 属性实际具有其值的有效电话号码。

使用其基本配置时，语法验证（如模式检查）将检查任何目录修改，以确保属性值与所需语法匹配，并将拒绝违反语法的任何修改。（可选）可以将语法验证配置为记录有关语法违反情况的警告消息，并拒绝更改或允许修改过程成功。

除 DN 外，所有语法都根据 RFC 4514 进行验证。默认情况下，DN 会根据 RFC 1779 或 RFC 2253 进

行验证，这比 RFC 4514 低。必须明确配置 DN 的严格验证。

此功能检查所有属性语法，但二进制语法（无法验证）和非标准语法（没有定义的必要格式）除外。未验证的 语法如下：

- 传真（二进制）
- OctetString (binary)
- JPEG (binary)
- 二进制（非标准）
- 空格代表敏感字符串（非标准）
- URI （非标准）

启用语法验证后，每当向条目中添加或修改属性时，都会检查 新的 属性值。（这不包括 复制 更改，因为在供应商服务器上检查语法。）

第 8 章 条目属性参考

此引用中列出的属性手动分配或提供给目录条目。属性按字母顺序列出，其定义、语法和 OID。

8.1. ABSTRACT

abstract 属性包含文档条目的抽象。

OID	0.9.2342.19200300.102.1.9
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Internet White Pages Pilot

8.2. ACCESSTO

此属性定义允许用户访问的特定主机或服务器。

OID	5.3.6.1.1.1.1.1
语法	IA5String
multi- 或 Single-Valued	多值
定义在	nss_ldap/pam_ldap

8.3. ACCOUNTINACTIVITYLIMIT

accountInactivityLimit 属性设置帐户最后一次登录时间（以秒为单位）。

OID	1.3.6.1.4.1.11.1.3.2.1.3
语法	DirectoryString
multi- 或 Single-Valued	单值

定义在	目录服务器

8.4. ACCTPOLICYSUBENTRY

acctPolicySubentry 属性标识属于帐户策略的任何条目（特别是帐户锁定策略）。此属性的值指向应用到该条目的帐户策略。

这可以在单独的用户条目或 CoS 模板条目或角色条目上设置。

OID	1.3.6.1.4.1.11.1.3.2.1.2
语法	DN
multi- 或 Single-Valued	单值
定义在	目录服务器

8.5. ADMINISTRATORCONTACTINFO

此属性包含 LDAP 或服务器管理员的联系信息。

OID	2.16.840.1.113730.3.1.74
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape 管理服务

8.6. ADMINROLE

此属性包含分配给条目中标识的用户的角色。

OID	2.16.840.1.113730.3.1.601
语法	DirectoryString
multi- 或 Single-Valued	单值

定义在	Netscape 管理服务

8.7. ADMINURL

此属性包含管理服务器的 URL。

OID	2.16.840.1.113730.3.1.75
语法	IA5String
multi- 或 Single-Valued	多值
定义在	Netscape 管理服务

8.8. ALIASEDOBJECTNAME

Directory 服务器使用 aliasedObjectName 属性来识别别名条目。此属性包含该条目的条目的 DN（区分名称）。例如：

```
aliasedObjectName: uid=jdoe,ou=people,dc=example,dc=com
```

OID	2.5.4.1
语法	DN
multi- 或 Single-Valued	单值
定义在	RFC 2256

8.9. ASSOCIATEDDOMAIN

associatedDomain 属性包含与目录树中的条目关联的 DNS 域。例如，带有可分辨名称 c=US,o=Example Corporation 的条目有相关的 EC.US 域。这些域应当以 RFC 822 顺序表示。

```
associatedDomain:US
```

OID	0.9.2342.19200300.100.1.37
语法	DirectoryString

multi- 或 Single-Valued	多值
定义在	RFC 1274

8.10. ASSOCIATEDNAME

associatedName 标识与 DNS 域关联的机构目录树条目。例如：

> ***associatedName: c=us***

OID	0.9.2342.19200300.100.1.38
语法	DN
multi- 或 Single-Valued	多值
定义在	RFC 1274

8.11. ATTRIBUTETYPES

此属性用于模式文件来识别 subschema 中定义的属性。

OID	2.5.21.5
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2252

8.12. AUDIO

audio 属性包含一个使用二进制格式的声音文件。此属性使用 u-law 编码的声音数据。例如：

> ***audio:: AAAAAA==***

OID	0.9.2342.19200300.100.1.55
语法	二进制

multi- 或 Single-Valued	多值
定义在	RFC 1274

8.13. AUTHORCN

authorCn 属性包含文档作者的通用名称。例如：

```
authorCn: John Smith
```

OID	0.9.2342.19200300.102.1.11
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Internet White Pages Pilot

8.14. AUTHORITYREVOCATIONLIST

authorityRevocationList 属性包含已撤销的 CA 证书的列表。此属性应以二进制格式请求并存储，如 authorityRevocationList;binary。例如：

```
authorityrevocationlist;binary:: AAAAAA==
```

OID	2.5.4.38
语法	二进制
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.15. AUTHORSN

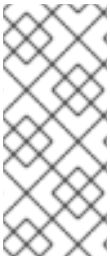
authorSn 属性包含文档条目的作者姓氏或系列名称。例如：

```
authorSn: Smith
```

OID	0.9.2342.19200300.102.1.12
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Internet White Pages Pilot

8.16. AUTOMOUNTINFORMATION

此属性包含 autofs 自动挂载程序使用的信息。



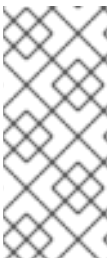
注意

automountInformation 属性在目录服务器中的 60autofs.ldif 中定义。要使用更新的 RFC 2307 模式，请删除 60autofs.ldif 文件，并将 10rfc2307bis.ldif 文件从 /usr/share/dirsrv/data 目录复制到 /etc/dirsrv/slapd-实例/schema 目录。

OID	1.3.6.1.1.1.1.33
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	RFC 2307

8.17. BOOTFILE

此属性包含引导镜像文件名。



注意

bootFile 属性在目录服务器中的 10rfc2307.ldif 中定义。要使用更新的 RFC 2307 模式，请删除 10rfc2307.ldif 文件，并将 10rfc2307bis.ldif 文件从 /usr/share/dirsrv/data 目录复制到 /etc/dirsrv/slapd-instance/schema 目录。

OID	1.3.6.1.1.1.1.24

语法	IA5String
multi- 或 Single-Valued	多值
定义在	RFC 2307

8.18. BOOTPARAMETER

此属性包含 rpc.bootparamd 的值。

注意

bootParameter 属性在目录服务器中的 10rfc2307.ldif 中定义。要使用更新的 RFC 2307 模式，请删除 10rfc2307.ldif 文件，并将 10rfc2307bis.ldif 文件从 /usr/share/dirsrv/data 目录复制到 /etc/dirsrv/slapd-instance/schema 目录。

OID	1.3.6.1.1.1.1.23
语法	IA5String
multi- 或 Single-Valued	多值
定义在	RFC 2307

8.19. BUILDINGNAME

build Name 属性包含与条目关联的构建名称。例如：

```
buildingName: 14
```

OID	0.9.2342.19200300.100.1.48
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 1274

8.20. BUSINESSCATEGORY

businessCategory 属性标识条目参与的商业类型。属性值应该是广泛的常规化，如企业部门级别。例如：

```
businessCategory: Engineering
```

OID	2.5.4.15
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.21. CACERTIFICATE

cACertificate 属性包含一个 CA 证书。该属性应请求并存储二进制格式，如 cACertificate;binary。例如：

```
cACertificate;binary:: AAAAAA==
```

OID	2.5.4.37
语法	二进制
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.22. C

countryName 或 c 属性包含表示国家名称的双字符国家代码。国家/地区代码由 ISO 定义。例如：

```
countryName: GB
c: US
```

OID	2.5.4.6
语法	DirectoryString
multi- 或 Single-Valued	单值

定义在	RFC 2256

8.23. CARLICENSE

carLicense 属性包含一个条目的 automobile 许可证的数量。例如：

```
carLicense: 6ABC246
```

OID	2.16.840.1.113730.3.1.1
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2798

8.24. CERTIFICATEREVOCATIONLIST

certificateRevocationList 属性包含撤销的用户证书的列表。要请求属性值并以二进制形式存储，作为 certificateACertificate;binary。例如：

```
certificateRevocationList;binary:: AAAAAA==
```

OID	2.5.4.39
语法	二进制
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.25. CN

commonName 属性包含条目的名称。对于用户条目，cn 属性通常是个人的完整名称。例如：

```
commonName: John Smith
cn: Bill Anderson
```

使用 LDAPReplica 或 LDAPServerobject 对象类时，cn 属性值具有以下格式：

```
cn: replicater.example.com:17430/dc%3Dexample%2Cdc%3com
```

OID	2.5.4.3
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.26. CO

friendlyCountryName 属性包含国家名称；这可以是任意字符串。通常，国家 /地区与 ISO 指定的双字母国家代码一起使用，而 co 属性包含可读的国家名称。例如：

```
friendlyCountryName: Ireland
co: Ireland
```

OID	0.9.2342.19200300.100.1.43
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 1274

8.27. COSATTRIBUTE

cosAttribute 包含为 CoS 生成值的属性名称。可以指定多个 cosAttribute 值。此属性被所有类型的 CoS 定义条目使用。

OID	2.16.840.1.113730.3.1.550
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	目录服务器

8.28. COSINDIRECTSPECIFIER

cosIndirectSpecifier 指定间接 CoS 用于识别模板条目的属性值。

OID	2.16.840.1.113730.3.1.577
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	目录服务器

8.29. COSPRIORITY

cosPriority 属性指定在 CoS 模板竞争提供属性值时，哪个模板提供属性值。此属性代表模板的全局优先级。优先级为零是最高优先级。

OID	2.16.840.1.113730.3.1.569
语法	整数
multi- 或 Single-Valued	单值
定义在	目录服务器

8.30. COSSPECIFIER

cosSpecifier 属性包含经典 CoS 使用的属性值，该属性以及模板条目的 DN，用于标识模板条目。

OID	2.16.840.1.113730.3.1.551
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	目录服务器

8.31. COSTARGETTREE

cosTargetTree 属性定义 CoS 模式应用到的子树。schema 和多个 CoS 模式此属性的值可能会随机重叠其目标树。

OID	2.16.840.1.113730.3.1.552
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	目录服务器

8.32. COSTEMPLATEDN

cosTemplateDn 属性包含模板条目的 DN，其中包含共享属性值的列表。对模板条目属性值的更改会自动应用到 CoS 范围内的所有条目。单个 CoS 可能有多个与它关联的模板条目。

OID	2.16.840.1.113730.3.1.553
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	目录服务器

8.33. CROSSCERTIFICATEPAIR

必须请求 crossCertificatePair 属性的值，并以二进制格式存储，如 certificateCertificateRepair;binary。例如：

```
crossCertificatePair;binary:: AAAAAA==
```

OID	2.5.4.40
语法	二进制
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.34. DC

dc 属性包含域名的一个组件。例如：

```
dc: example
domainComponent: example
```

OID	0.9.2342.19200300.100.1.25
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	RFC 2247

8.35. DELTAREVOCATIONLIST

deltaRevocationList 属性包含一个证书撤销列表(CRL)。属性值以二进制格式请求并存储，如 deltaRevocationList;binary。

OID	2.5.4.53
语法	二进制
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.36. DEPARTMENTNUMBER

departmentNumber 属性包含一个条目的部门号。例如：

```
departmentNumber: 2604
```

OID	2.16.840.1.113730.3.1.2
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2798

8.37. DESCRIPTION

description 属性为条目提供人类可读的描述。对于 个人或 组织 对象类，这可用于条目的角色或工作分配。例如：

> *description: Quality control inspector for the ME2873 product line.*

OID	2.5.4.13
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.38. DESTINATIONINDICATOR

destinationIndicator 属性包含与条目关联的城市和国家/地区。此属性是提供公共的 telegram 服务，通常与 registeredAddress 属性一起使用。例如：

> *destinationIndicator: Stow, Ohio, USA*

OID	2.5.4.27
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.39. DISPLAYNAME

displayName 属性包含显示该个人条目时要使用的个人的首选名称。这对在一行摘要列表中显示条目的首选名称特别有用。因为其他属性类型（如 cn ）是多值，所以它们无法用来显示首选名称。例如：

> *displayName: John Smith*

OID	2.16.840.1.113730.3.1.241
语法	DirectoryString

multi- 或 Single-Valued	单值
定义在	RFC 2798

8.40. DITREDIRECT

dITRedirect 属性表示一个条目描述的对象现在在目录树中有一个较新的条目。当个人的工作更改时，可以使用此属性，单独获取新的组织 DN。

> *dITRedirect: cn=jsmith,dc=example,dc=com*

OID	0.9.2342.19200300.100.1.54
语法	DN
定义在	RFC 1274

8.41. DMDNAME

dmdName 属性值指定一个目录管理域(DMD)，这是运行 Directory Server 的管理授权。

OID	2.5.4.54
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	RFC 2256

8.42. DN

dn 属性包含一个条目的可分辨名称。例如：

> *dn: uid=Barbara Jensen,ou=Quality Control,dc=example,dc=com*

OID	2.5.4.49
语法	DN

定义在	RFC 2256

8.43. DNSRECORD

dNSRecord 属性包含 DNS 资源记录，包括类型 A （地址）、类型 MX （邮件交换）、类型 NS （名称服务器）以及类型 SOA （授权起始）资源记录。例如：

> *dNSRecord: IN NS ns.uu.net*

OID	0.9.2342.19200300.100.1.26
语法	IA5String
multi- 或 Single-Valued	多值
定义在	Internet Directory Pilot

8.44. DOCUMENTAUTHOR

documentAuthor 属性包含文档条目的作者 DN。例如：

> *documentAuthor: uid=Barbara Jensen,ou=People,dc=example,dc=com*

OID	0.9.2342.19200300.100.1.14
语法	DN
multi- 或 Single-Valued	多值
定义在	RFC 1274

8.45. DOCUMENTIDENTIFIER

documentIdentifier 属性包含文档的唯一标识符。例如：

> *documentIdentifier: L3204REV1*

OID	0.9.2342.19200300.100.1.11

语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 1274

8.46. DOCUMENTLOCATION

documentLocation 属性包含文档原始版本的位置。例如：

> ***documentLocation: Department Library***

OID	0.9.2342.19200300.100.1.15
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 1274

8.47. DOCUMENTPUBLISHER

documentPublisher 属性包含发布文档的人员或机构。例如：

> ***documentPublisher: Southeastern Publishing***

OID	0.9.2342.19200300.100.1.56
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	RFC 1274

8.48. DOCUMENTSTORE

documentStore 属性包含有关存储文档的信息。

OID	0.9.2342.19200300.102.1.10

语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Internet White Pages Pilot

8.49. DOCUMENTTITLE

documentTitle 属性包含文档的标题。例如：

```
documentTitle: Installing Red Hat Directory Server
```

OID	0.9.2342.19200300.100.1.12
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 1274

8.50. DOCUMENTVERSION

documentVersion 属性包含文档的当前版本号。例如：

```
documentVersion: 1.1
```

OID	0.9.2342.19200300.100.1.13
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 1274

8.51. DRINK

favouriteDrink 属性包含个人最喜欢的信用。这可以缩短为 drink。例如：

> ***favouriteDrink: iced tea***
> ***drink: cranberry juice***

OID	0.9.2342.19200300.100.1.5
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 1274

8.52. DSAQUALITY

dSAQuality 属性包含目录系统代理(DSA)质量的评级。此属性允许 DSA 管理器指示 DSA 的预期可用性级别。例如：

> ***dSAQuality: high***

OID	0.9.2342.19200300.100.1.49
语法	directory-String
multi- 或 Single-Valued	单值
定义在	RFC 1274

8.53. EMPLOYEENUMBER

employeeNumber 属性包含个人的员工数量。例如：

> ***employeeNumber: 3441***

OID	2.16.840.1.113730.3.1.3
语法	directory-String
multi- 或 Single-Valued	单值
定义在	RFC 2798

8.54. EMPLOYEETYPE

employeeType 属性包含个人的雇佣类型。例如：

```
employeeType: Full time
```

OID	2.16.840.1.113730.3.1.4
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2798

8.55. ENHANCEDSEARCHGUIDE

enhancedSearchGuide 属性包含 X.500 客户端用来构造搜索过滤器的信息。例如：

```
enhancedSearchGuide: (uid=bjensen)
```

OID	2.5.4.47
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2798

8.56. FAX

facsimileTelephoneNumber 属性包含条目的 facsimile 编号；此属性可以缩写为 fax。例如：

```
facsimileTelephoneNumber: +1 415 555 1212
fax: +1 415 555 1212
```

OID	2.5.4.23
语法	telephoneNumber
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.57. GECOS

gecos 属性用于确定用户的 GECOS 字段。这与 cn 属性类似，但使用 gecos 属性允许将其他信息嵌入到来自通用名称的 GECOS 字段中。如果目录中存储的通用名称不是用户的全名，则此字段也很有用。

```
gecos: John Smith
```

注意

gecos 属性在目录服务器中的 10rfc2307.ldif 中定义。要使用更新的 RFC 2307 模式，请删除 10rfc2307.ldif 文件，并将 10rfc2307bis.ldif 文件从 /usr/share/dirsrv/data 目录复制到 /etc/dirsrv/slapd-instance/schema 目录。

OID	1.3.6.1.1.1.1.2
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	RFC 2307

8.58. GENERATIONQUALIFIER

generationQualifier 属性包含个人名称的生成限定符，这通常作为名称的后缀附加。例如：

```
generationQualifier:III
```

OID	2.5.4.44
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.59. GIDNUMBER

gidNumber 属性包含组条目的唯一数字标识符，或者标识用户条目的组。这与 Unix 中的组号类似。

```
gidNumber: 100
```

注意

gidNumber 属性在目录服务器中的 10rfc2307.ldif 中定义。要使用更新的 RFC 2307 模式，请删除 10rfc2307.ldif 文件，并将 10rfc2307bis.ldif 文件从 /usr/share/dirsrv/data 目录复制到 /etc/dirsrv/slapd-instance/schema 目录。

OID	1.3.6.1.1.1.1.1
语法	整数
multi- 或 Single-Valued	单值
定义在	RFC 2307

8.60. GIVENNAME

givenName 属性包含一个条目的给定名称，通常是名字。例如：

```
givenName: Rachel
```

OID	2.5.4.42
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.61. HOMEDIRECTORY

homeDirectory 属性包含用户主目录的路径。

```
homeDirectory: /home/jsmith
```

注意

homeDirectory 属性在目录服务器中的 10rfc2307.ldif 中定义。要使用更新的 RFC 2307 模式，请删除 10rfc2307.ldif 文件，并将 10rfc2307bis.ldif 文件从 /usr/share/dirsrv/data 目录复制到 /etc/dirsrv/slapd-instance/schema 目录。

OID	1.3.6.1.1.1.1.3
语法	IA5String
multi- 或 Single-Valued	单值
定义在	RFC 2307

8.62. HOMEPHONE

homePhone 属性包含条目的托管电话号码。例如：

```
homePhone: 415-555-1234
```

注意

虽然 RFC 1274 同时将 homeTelephoneNumber 和 homePhone 定义为 residential 电话号码属性的名称，但目录服务器仅实施 homePhone 名称。

OID	0.9.2342.19200300.100.1.20
语法	telephoneNumber
multi- 或 Single-Valued	多值
定义在	RFC 1274

8.63. HOMEPOSTALADDRESS

homePostalAddress 属性包含一个条目的主邮件地址。由于此属性通常跨越多行，因此每个换行符都必须以美元符号($)表示。要在属性值中代表实际美元符号($)或反斜杠(\)，请分别使用转义的十六进制值 \24 和 \5c。例如：

```
homePostalAddress: 1234 Ridgeway Drive$Santa Clara, CA$99555
```

- *代表以下字符串：*

> ***The dollar ($) value can be found in the c:\cost file.***

entry 值为：

> ***The dollar (\24) value can be found$in the c:\c5cost file.***

OID	0.9.2342.19200300.100.1.39
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 1274

8.64. 主机

主机 包含计算机的主机名。例如：

> ***host: labcontroller01***

OID	0.9.2342.19200300.100.1.9
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 1274

8.65. HOUSEIDENTIFIER

houseIdentifier 包含位置上特定构建的标识符。例如：

> ***houseIdentifier: B105***

OID	2.5.4.51

语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.66. INETDOMAINBASEDN

此属性标识 DNS 域的用户子树的基本 DN。

OID	2.16.840.1.113730.3.1.690
语法	DN
multi- 或 Single-Valued	单值
定义在	订阅者互操作性

8.67. INETDOMAINSTATUS

此属性显示域的当前状态。域的状态为 active、active 或删除。

OID	2.16.840.1.113730.3.1.691
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	订阅者互操作性

8.68. INETSUBSCRIBERACCOUNTID

此属性包含唯一属性，用于将订阅者的用户条目链接到计费系统。

OID	2.16.840.1.113730.3.1.694
语法	DirectoryString
multi- 或 Single-Valued	多值

定义在	订阅者互操作性

8.69. INETSUBSCRIBERCHALLENGE

inetSubscriberChallenge 属性包含某种问题或提示，即质询短语，用于确认 subscriberIdentity 属性中的用户的身份。此属性与 inetSubscriberResponse 属性结合使用，其中包含对质询的响应。

OID	2.16.840.1.113730.3.1.695
语法	IA5String
multi- 或 Single-Valued	单值
定义在	订阅者互操作性

8.70. INETSUBSCRIBERRESPONSE

inetSubscriberResponse 属性包含 inetSubscriberChallenge 属性中质询问题的回答，以验证 subscriberIdentity 属性中的用户。

OID	2.16.840.1.113730.3.1.696
语法	IA5String
multi- 或 Single-Valued	多值
定义在	订阅者互操作性

8.71. INETUSERHTTPURL

此属性包含与用户关联的 Web 地址。

OID	2.16.840.1.113730.3.1.693
语法	IA5String
multi- 或 Single-Valued	多值
定义在	订阅者互操作性

8.72. INETUSERSTATUS

此属性显示用户的当前状态(subscriber)。用户的状态为 active、active 或删除。

OID	2.16.840.1.113730.3.1.692
语法	DirectoryString
multi- 或 Single-Valued	single-Valued
定义在	订阅者互操作性

8.73. INFO

info 属性包含有关对象的任何常规信息。避免将此属性用于特定信息，并依赖特定的（可能自定义）属性类型。例如：

```
info: not valid
```

OID	0.9.2342.19200300.100.1.4
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 1274

8.74. 初始

初始版本 包含个人的首字母；这不包含条目的 surname。例如：

```
initials: BAJ
```

目录服务器和 Active Directory 以不同的方式处理 initials 属性。目录服务器允许实际数量无限的字符，而 Active Directory 则限制六个字符。如果条目与 Windows peer 同步，并且 initials 属性的值超过 6 个字符，则该值会在同步时自动截断为六个字符。没有写入错误日志的信息，以指示同步更改了属性值。

OID	2.5.4.43

语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.75. INSTALLATIONTIMESTAMP

这包括安装服务器实例的时间。

OID	2.16.840.1.113730.3.1.73
语法	DirectoryString
multi- 或 Single-Valued	multi-Valued
定义在	Netscape 管理服务

8.76. INTERNATIONALISDNNUMBER

internationalISDNNumber 属性包含文档条目的 ISDN 数。此属性使用在 CCITT Rec 中给定的 ISDN 地址的国际识别格式。E.164.

OID	2.5.4.25
语法	IA5String
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.77. IPHOSTNUMBER

它包含服务器的 IP 地址。

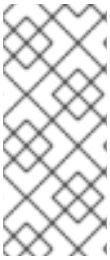
注意

ipHostNumber 属性在目录服务器中的 10rfc2307.ldif 中定义。要使用更新的 RFC 2307 模式，请删除 10rfc2307.ldif 文件，并将 10rfc2307bis.ldif 文件从 /usr/share/dirsrv/data 目录复制到 /etc/dirsrv/slapd-instance/schema 目录。

OID	1.3.6.1.1.1.1.19
语法	DirectoryString
multi- 或 Single-Valued	multi-Valued
定义在	RFC 2307

8.78. IPNETMASKNUMBER

它包含服务器的 IP 子网掩码。



注意

ipHostNumber 属性在目录服务器中的 10rfc2307.ldif 中定义。要使用更新的 RFC 2307 模式，请删除 10rfc2307.ldif 文件，并将 10rfc2307bis.ldif 文件从 /usr/share/dirsrv/data 目录复制到 /etc/dirsrv/slapd-instance/schema 目录。

OID	2.16.840.1.113730.3.1.73
语法	DirectoryString
multi- 或 Single-Valued	multi-Valued
定义在	RFC 2307

8.79. IPNETWORKNUMBER

这可标识 IP 网络。

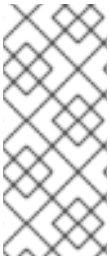
注意

ipNetworkNumber 属性在目录服务器中的 10rfc2307.ldif 中定义。要使用更新的 RFC 2307 模式，请删除 10rfc2307.ldif 文件，并将 10rfc2307bis.ldif 文件从 /usr/share/dirsrv/data 目录复制到 /etc/dirsrv/slapd-instance/schema 目录。

OID	1.3.6.1.1.1.1.20
语法	DirectoryString
multi- 或 Single-Valued	single-Valued
定义在	RFC 2307

8.80. IPPROTOCOLNUMBER

此属性标识 IP 协议版本号。



注意

ipProtocolNumber 属性在目录服务器中的 10rfc2307.ldif 中定义。要使用更新的 RFC 2307 模式，请删除 10rfc2307.ldif 文件，并将 10rfc2307bis.ldif 文件从 /usr/share/dirsrv/data 目录复制到 /etc/dirsrv/slapd-instance/schema 目录。

OID	1.3.6.1.1.1.1.17
语法	整数
multi- 或 Single-Valued	single-Valued
定义在	RFC 2307

8.81. IPSERVICEPORT

此属性提供 IP 服务使用的端口。

注意

ipServicePort 属性在目录服务器中的 10rfc2307.ldif 中定义。要使用更新的 RFC 2307 模式，请删除 10rfc2307.ldif 文件，并将 10rfc2307bis.ldif 文件从 /usr/share/dirsrv/data 目录复制到 /etc/dirsrv/slapd-instance/schema 目录。

OID	1.3.6.1.1.1.1.15
语法	整数
multi- 或 Single-Valued	single-Valued
定义在	RFC 2307

8.82. IPSERVICEPROTOCOL

这可标识 IP 服务使用的协议。

注意

ipServiceProtocol 属性在目录服务器中的 10rfc2307.ldif 中定义。要使用更新的 RFC 2307 模式，请删除 10rfc2307.ldif 文件，并将 10rfc2307bis.ldif 文件从 /usr/share/dirsrv/data 目录复制到 /etc/dirsrv/slapd-instance/schema 目录。

OID	1.3.6.1.1.1.1.16
语法	DirectoryString
multi- 或 Single-Valued	multi-Valued
定义在	RFC 2307

8.83. JANETMAILBOX

janetMailbox 包含 JANET 电子邮件地址，通常为位于英国的用户，不使用 RFC 8822 电子邮件地址。具有此属性的条目还必须包含 rfc822Mailbox 属性。

OID	0.9.2342.19200300.100.1.46

语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 1274

8.84. JPEGPHOTO

jpegPhoto 属性包含二进制值的 JPEG 照片。例如：

```
jpegPhoto:: AAAAAA==
```

OID	0.9.2342.19200300.100.1.60
语法	二进制
multi- 或 Single-Valued	多值
定义在	RFC 2798

8.85. KEYWORDS

keyWord 属性包含与条目关联的关键字。例如：

```
keyWords: directory LDAP X.500
```

OID	0.9.2342.19200300.102.1.7
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Internet White Pages Pilot

8.86. KNOWLEDGEINFORMATION

不再使用此属性。

OID	2.5.4.2

语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.87. LABELEDURI

labeledURI 包含与条目相关的统一资源标识符(URI)。放置在属性中的值应由 URI 组成（当前只支持 URL），可选后跟一个或多个空格字符和标签。

```
labeledURI: http://home.example.com
labeledURI: http://home.example.com Example website
```

OID	1.3.6.1.4.1.250.1.57
语法	IA5String
multi- 或 Single-Valued	多值
定义在	RFC 2709

8.88. L

localityName 或 l, 属性包含与条目关联的计数、城市或其他地理设计。例如：

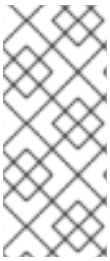
```
localityName: Santa Clara
l: Santa Clara
```

OID	2.5.4.7
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.89. LOGINSHELL

loginShell 属性包含用户登录域时自动启动的脚本的路径。

loginShell: c:\scripts\jsmith.bat



注意

loginShell 属性在目录服务器中的 10rfc2307.ldif 中定义。要使用更新的 RFC 2307 模式，请删除 10rfc2307.ldif 文件，并将 10rfc2307bis.ldif 文件从 /usr/share/dirsrv/data 目录复制到 /etc/dirsrv/slapd-instance/schema 目录。

OID	1.3.6.1.1.1.1.4
语法	IA5String
multi- 或 Single-Valued	单值
定义在	RFC 2307

8.90. MACADDRESS

此属性提供服务器或设备的 MAC 地址。

注意

macAddress 属性在目录服务器中的 10rfc2307.ldif 中定义。要使用更新的 RFC 2307 模式，请删除 10rfc2307.ldif 文件，并将 10rfc2307bis.ldif 文件从 /usr/share/dirsrv/data 目录复制到 /etc/dirsrv/slapd-instance/schema 目录。

OID	1.3.6.1.1.1.1.22
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2307

8.91. MAILACCESSDOMAIN

此属性列出了用户可用于访问消息传递服务器的域。

OID	2.16.840.1.113730.3.1.12
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape Messaging Server

8.92. MAIL

mail 属性包含用户的主电子邮件地址。此属性值由白色页面应用程序检索并显示。例如：

> ***mail: jsmith@example.com***

OID	0.9.2342.19200300.100.1.3
语法	DirectyString
multi- 或 Single-Valued	单值
定义在	RFC 1274

8.93. MAILALTERNATEADDRESS

mailAlternateAddress 属性包含用户的额外电子邮件地址。此属性不反映默认或主要电子邮件地址；该电子邮件地址由 mail 属性设置。

例如：

> ***mailAlternateAddress: jsmith@example.com***
> ***mailAlternateAddress: smith1701@alt.com***

OID	2.16.840.1.113730.3.1.13
语法	DirectyString
multi- 或 Single-Valued	多值
定义在	RFC 1274

8.94. MAILAUTOREPLYMODE

此属性设定是否为消息传递服务器启用自动回复。

OID	2.16.840.1.113730.3.1.14
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape Messaging Server

8.95. MAILAUTOREPLYTEXT

此属性存储要在自动回复电子邮件中使用的文本。

OID	2.16.840.1.113730.3.1.15
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape Messaging Server

8.96. MAILDELIVERYOPTION

此属性定义用于 mail 用户的邮件发送机制。

OID	2.16.840.1.113730.3.1.16
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape Messaging Server

8.97. MAILENHANCEDUNIQUEMEMBER

此属性包含邮件组的唯一成员的 DN。

OID	2.16.840.1.113730.3.1.31
语法	DN
multi- 或 Single-Valued	多值
定义在	Netscape Messaging Server

8.98. MAILFORWARDINGADDRESS

此属性包含一个将用户电子邮件转发到的电子邮件地址。

OID	2.16.840.1.113730.3.1.17
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape Messaging Server

8.99. MAILHOST

mailHost 属性包含邮件服务器的主机名。例如：

```
mailHost: mail.example.com
```

OID	2.16.840.1.113730.3.1.18
语法	DirectyString
multi- 或 Single-Valued	多值
定义在	Netscape Messaging Server

8.100. MAILMESSAGESTORE

这可标识用户电子邮件框的位置。

OID	2.16.840.1.113730.3.1.19
语法	IA5String
multi- 或 Single-Valued	多值
定义在	Netscape Messaging Server

8.101. MAILPREFERENCEOPTION

mailPreferenceOption 定义是否将用户包含在电子邮件列表（电子邮件和物理上）中。有三个选项：

0	不出现在邮件列表中。
1	将 添加到任何邮件列表中。
2	仅添加到与用户兴趣相关的供应商视图的 mailing 列表中。

如果属性不存在，则默认为 假定用户不包含在任何邮件列表中。此属性应该由使用目录的用户解释，以派生邮件列表及其值。例如：

```
mailPreferenceOption: 0
```

OID	0.9.2342.19200300.100.1.47
语法	整数
multi- 或 Single-Valued	单值
定义在	RFC 1274

8.102. MAILPROGRAMDELIVERYINFO

此属性包含用于编程邮件发送的任何命令。

OID	2.16.840.1.113730.3.1.20
语法	IA5String
multi- 或 Single-Valued	多值
定义在	Netscape Messaging Server

8.103. MAILQUOTA

此属性设定用户邮件框允许的磁盘空间量。

OID	2.16.840.1.113730.3.1.21
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape Messaging Server

8.104. MAILROUTINGADDRESS

此属性包含在将用户接收的电子邮件转发到另一个消息传递服务器时要使用的路由地址。

OID	2.16.840.1.113730.3.1.24
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape Messaging Server

8.105. MANAGER

管理器 包含个人的管理器的可分辨名称(DN)。例如：

```
manager: cn=Bill Andersen,ou=Quality Control,dc=example,dc=com
```

OID	0.9.2342.19200300.100.1.10

语法	DN
multi- 或 Single-Valued	多值
定义在	RFC 1274

8.106. 成员

member 属性包含组的每个成员的可分辨名称(DN)。例如：

```
member: cn=John Smith,dc=example,dc=com
```

OID	2.5.4.31
语法	DN
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.107. MEMBERCERTIFICATEDESCRIPTION

此属性是一个多值属性，其中每个值都是描述、模式或过滤器，与证书的主题 DN 匹配，通常是用于 TLS 客户端身份验证的证书。

memberCertificateDescription 与包含主题 DN 的任何证书匹配，其属性-值断言(AVAs)作为描述。描述可以包含多个 ou AVAs。匹配的 DN 必须包含它们相同的 ou AVAs，但可能与其他 AVAs 进行交互，包括其他 ou AVAs。对于任何其他属性类型（而不是 ou），描述中最多应该有一个 AVA 类型。如果有多个，则忽略所有，但最后一个操作都会被忽略。

匹配的 DN 必须包含相同的 AVA，但没有其它同类型的 AVA，但完全没有其他同类型的 AVA （扁平、语法方式）。

如果 AVAs 包含相同的属性描述（区分大小写的比较）和相同的属性值（不区分大小写的比较、前导和尾随空格忽略，并且连续的空格字符被视为单个空格），则它们被视为相同。

要被视为具有以下 memberCertificateDescription 值的组的成员，证书需要包含 ou=x、ou=A 和 dc=example，但不包括 dc=company。

memberCertificateDescription: {ou=x,ou=A,dc=company,dc=example}

要匹配组的要求，证书的主题 DN 必须包含与 memberCertificateDescription 属性中定义的相同 ou 属性类型。

OID	2.16.840.1.113730.3.1.199
语法	IA5String
multi- 或 Single-Valued	多值
定义在	目录服务器

8.108. MEMBERNISNETGROUP

此属性通过列出合并 netgroup 的名称，将另一个 netgroup 的属性值合并到当前组中。

注意

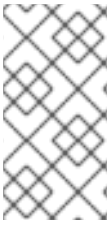
memberNisNetgroup 属性在 Directory Server 中的 10rfc2307.ldif 中定义。要使用更新的 RFC 2307 模式，请删除 10rfc2307.ldif 文件，并将 10rfc2307bis.ldif 文件从 /usr/share/dirsrv/data 目录复制到 /etc/dirsrv/slapd-instance/schema 目录。

OID	1.3.6.1.1.1.1.13
语法	IA5String
multi- 或 Single-Valued	多值
定义在	RFC 2307

8.109. MEMBEROF

此属性包含用户所属的组名称。

memberOf 是组成员的用户条目上的 MemberOf 插件生成的默认属性。此属性自动同步到组条目中列出的 成员属性，以便显示条目的组成员资格由 Directory Server 管理。



注意

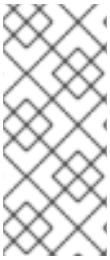
只有在启用了 MemberOf 插件并且配置为使用此属性时，此属性仅在组条目和相应成员的用户条目之间同步。

OID	1.2.840.113556.1.2.102
语法	DN
multi- 或 Single-Valued	多值
定义在	Netscape 委派管理员

8.110. MEMBERUID

memberUid 属性包含组成员的登录名称；这与 member 属性中标识的 DN 不同。

```
memberUID: jsmith
```



注意

memberUID 属性在目录服务器中的 10rfc2307.ldif 中定义。要使用更新的 RFC 2307 模式，请删除 10rfc2307.ldif 文件，并将 10rfc2307bis.ldif 文件从 /usr/share/dirsrv/data 目录复制到 /etc/dirsrv/slapd-instance/schema 目录。

OID	1.3.6.1.1.1.1.12
语法	IA5String
multi- 或 Single-Valued	单值
定义在	RFC 2307

8.111. MEMBERURL

此属性标识与组的每个成员关联的 URL。可以使用任何类型的标记的 URL。

```
memberURL: ldap://cn=jsmith,ou=people,dc=example,dc=com
```

OID	2.16.840.1.113730.3.1.198
语法	IA5String
multi- 或 Single-Valued	多值
定义在	目录服务器

8.112. MEPMANAGEDBY

此属性包含自动生成的条目中的指针，指向原始条目的 DN。此属性由 Managed Entries 插件设置，无法手动修改。

OID	2.16.840.1.113730.3.1.2086
语法	DN
multi- 或 Single-Valued	单值
定义在	目录服务器

8.113. MEPMANAGEDENTRY

此属性包含一个指向自动生成的条目的指针，对应于当前条目。此属性由 Managed Entries 插件设置，无法手动修改。

OID	2.16.840.1.113730.3.1.2087
语法	DN
multi- 或 Single-Valued	单值
定义在	目录服务器

8.114. MEPMAPPEDATTR

此属性在 Managed Entries 模板条目中设置一个属性，该条目必须存在于生成的条目中。映射 意味着原始条目的一些值用于提供给定属性。这些属性的值将是令牌，格式为 attribute: $attr。例如：

```
mepMappedAttr: gidNumber: $gidNumber
```

只要属性扩展令牌的语法不违反所需的属性语法，就可以在 属性中使用其他术语和字符串。例如：

```
mepMappedAttr: cn: Managed Group for $cn
```

OID	2.16.840.1.113730.3.1.2089
语法	OctetString
multi- 或 Single-Valued	多值
定义在	目录服务器

8.115. MEPRDNATTR

此属性设置在由 Managed Entries 插件创建的自动生成的条目中将哪些属性用作 naming 属性。在 naming 属性中给定的任何属性 类型都 应以 mepMappedAttr 的形式存在于受管条目模板条目中。

OID	2.16.840.1.113730.3.1.2090
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	目录服务器

8.116. MEPSTATICATTR

此属性设置具有定义值的属性，该属性必须添加到由 Managed Entries 插件管理的自动生成的条目中。这个值将用于由 Managed Entries 插件的实例生成的每个条目。

```
mepStaticAttr: posixGroup
```

OID	2.16.840.1.113730.3.1.2088
语法	OctetString
multi- 或 Single-Valued	多值
定义在	目录服务器

8.117. MGRPADDHEADER

此属性包含有关消息中的标头的信息。

OID	2.16.840.1.113730.3.1.781
语法	IA5String
multi- 或 Single-Valued	多值
定义在	Netscape Messaging Server

8.118. MGRPALLOWEDBROADCASTER

此属性设置是否允许用户发送广播消息。

OID	2.16.840.1.113730.3.1.22
语法	IA5String
multi- 或 Single-Valued	多值
定义在	Netscape Messaging Server

8.119. MGRPALLOWEDDOMAIN

此属性设置邮件组的域。

OID	2.16.840.1.113730.3.1.23
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape Messaging Server

8.120. MGRPAPPROVEPASSWORD

此属性设置用户必须批准用于访问其电子邮件的密码。

OID	mgrpApprovePassword-oid
语法	IA5String
multi- 或 Single-Valued	单值
定义在	Netscape Messaging Server

8.121. MGRPBROADCASTERPOLICY

此属性定义广播电子邮件的策略。

OID	2.16.840.1.113730.3.1.788
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape Messaging Server

8.122. MGRPDELIVERTO

此属性包含有关电子邮件发送目的地的信息。

OID	2.16.840.1.113730.3.1.25
语法	IA5String
multi- 或 Single-Valued	多值
定义在	Netscape Messaging Server

8.123. MGRPERRORSTO

此属性包含有关为消息传递服务器发送错误消息的信息。

OID	2.16.840.1.113730.3.1.26
语法	IA5String
multi- 或 Single-Valued	单值
定义在	Netscape Messaging Server

8.124. MGRPMODERATOR

此属性包含邮件列表模式器的联系人名称。

OID	2.16.840.1.113730.3.1.33
语法	IA5String
multi- 或 Single-Valued	多值
定义在	Netscape Messaging Server

8.125. MGRPMSGMAXSIZE

此属性设置电子邮件消息允许的最大值。

OID	2.16.840.1.113730.3.1.32
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	Netscape Messaging Server

8.126. MGRPMSGREJECTACTION

此属性定义消息传递服务器应对被拒绝消息执行的操作。

OID	2.16.840.1.113730.3.1.28

语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape Messaging Server

8.127. MGRPMSGREJECTTEXT

此属性设置用于拒绝通知的文本。

OID	2.16.840.1.113730.3.1.29
语法	IA5String
multi- 或 Single-Valued	多值
定义在	Netscape Messaging Server

8.128. MGRPNODUPLICATECHECKS

此属性定义消息传递服务器是否检查重复电子邮件。

OID	2.16.840.1.113730.3.1.789
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	Netscape Messaging Server

8.129. MGRPREMOVEHEADER

此属性设置标头是否在回复信息中删除。

OID	2.16.840.1.113730.3.1.801
语法	DirectoryString
multi- 或 Single-Valued	多值

定义在	Netscape Messaging Server

8.130. MGRPRFC822MAILMEMBER

此属性标识邮件组的成员。

OID	2.16.840.1.113730.3.1.30
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape Messaging Server

8.131. 手机

手机 或 mobileTelephoneNumber 包含条目的手机或手机号码。例如：

```
mobileTelephoneNumber: 415-555-4321
```

OID	0.9.2342.19200300.100.1.41
语法	telephoneNumber
multi- 或 Single-Valued	多值
定义在	RFC 1274

8.132. MOZILLACUSTOM1

Mozilla Thunderbird 使用此属性来管理共享地址书。

OID	1.3.6.1.4.1.13769.4.1
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	Mozilla Address Book

8.133. MOZILLACUSTOM2

Mozilla Thunderbird 使用此属性来管理共享地址书。

OID	1.3.6.1.4.1.13769.4.2
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	Mozilla Address Book

8.134. MOZILLACUSTOM3

Mozilla Thunderbird 使用此属性来管理共享地址书。

OID	1.3.6.1.4.1.13769.4.3
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	Mozilla Address Book

8.135. MOZILLACUSTOM4

Mozilla Thunderbird 使用此属性来管理共享地址书。

OID	1.3.6.1.4.1.13769.4.4
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	Mozilla Address Book

8.136. MOZILLAHOMECOUNTRYNAME

此属性设置 Mozilla Thunderbird 在共享地址书中使用的国家/地区。

OID	1.3.6.1.4.1.13769.3.6
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	Mozilla Address Book

8.137. MOZILLAHOMELOCALITYNAME

此属性设置 Mozilla Thunderbird 在共享地址书中使用的城市。

OID	1.3.6.1.4.1.13769.3.3
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	Mozilla Address Book

8.138. MOZILLAHOMEPOSTALCODE

此属性设置 Mozilla Thunderbird 在共享地址书中使用的邮政代码。

OID	1.3.6.1.4.1.13769.3.5
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	Mozilla Address Book

8.139. MOZILLAHOMESTATE

此属性在共享地址书中设置 Mozilla Thunderbird 使用的状态或省时。

OID	1.3.6.1.4.1.13769.3.4
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	Mozilla Address Book

8.140. MOZILLAHOMESTREET2

此属性在共享地址书中包含 Mozilla Thunderbird 使用的 street 地址的第二行。

OID	1.3.6.1.4.1.13769.3.2
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	Mozilla Address Book

8.141. MOZILLAHOMESTREET

此属性设置 Mozilla Thunderbird 在共享地址书中使用的 street 地址。

OID	1.3.6.1.4.1.13769.3.1
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	Mozilla Address Book

8.142. MOZILLAHOMEURL

此属性包含 Mozilla Thunderbird 在共享地址书中使用的 URL。

OID	1.3.6.1.4.1.13769.3.7

语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	Mozilla Address Book

8.143. MOZILLANICKNAME

此属性包含 Mozilla Thunderbird 用于共享地址书的 nickname。

OID	1.3.6.1.4.1.13769.2.1
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Mozilla Address Book

8.144. MOZILLASECONDEMAIL

此属性在 Mozilla Thunderbird 的共享地址书中包含一个条目的备用或次要电子邮件地址。

OID	1.3.6.1.4.1.13769.2.2
语法	IA5String
multi- 或 Single-Valued	单值
定义在	Mozilla Address Book

8.145. MOZILLAUSEHTMLMAIL

此属性为 Mozilla Thunderbird 的共享地址书中的条目设置电子邮件类型首选项。

OID	1.3.6.1.4.1.13769.2.3
语法	布尔值
multi- 或 Single-Valued	单值

定义在	Mozilla Address Book

8.146. MOZILLAWORKSTREET2

此属性包含用于 Mozilla Thunderbird 共享地址》中的工作场所或办公室的树形地址。

OID	1.3.6.1.4.1.13769.3.8
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	Mozilla Address Book

8.147. MOZILLAWORKURL

此属性在 Mozilla Thunderbird 的共享地址书的条目中包含工作站点的 URL。

OID	1.3.6.1.4.1.13769.3.9
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	Mozilla Address Book

8.148. MULTILINEDESCRIPTION

此属性包含条目的描述，该条目跨越 LDIF 文件中的多行。

OID	1.3.6.1.4.1.250.1.2
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Internet White Pages Pilot

8.149. NAME

name 属性标识属性 supertype，可用于组成用于命名的字符串属性类型。

不太可能在条目中发生此类型的值。不支持属性子应用的 LDAP 服务器实现不需要在请求中识别此属性。客户端实施不应假设 LDAP 服务器能够执行属性子组。

OID	2.5.4.41
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.150. NETSCAPEREVERSIBLEPASSWORD

此属性包含 HTTP Digest/MD5 身份验证的密码。

OID	2.16.840.1.113730.3.1.812
语法	OctetString
multi- 或 Single-Valued	多值
定义在	Netscape Web Server

8.151. NISMAPENTRY

此属性包含供网络信息服务使用的 NIS 映射的信息。

注意

此属性在目录服务器中的 10rfc2307.ldif 中定义。要使用更新的 RFC 2307 模式，请删除 10rfc2307.ldif 文件，并将 10rfc2307bis.ldif 文件从 /usr/share/dirsrv/data 目录复制到 /etc/dirsrv/slapd-instance/schema 目录。

OID	1.3.6.1.1.1.1.27
语法	IA5String
multi- 或 Single-Valued	单值
定义在	RFC 2307

8.152. NISMAPNAME

此属性包含 NIS 服务器使用的映射的名称。

OID	1.3.6.1.1.1.1.26
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2307

8.153. NISNETGROUPTRIPLE

此属性包含 NIS 服务器使用的 netgroup 的信息。

注意

此属性在目录服务器中的 10rfc2307.ldif 中定义。要使用更新的 RFC 2307 模式，请删除 10rfc2307.ldif 文件，并将 10rfc2307bis.ldif 文件从 /usr/share/dirsrv/data 目录复制到 /etc/dirsrv/slapd-instance/schema 目录。

OID	1.3.6.1.1.1.1.14
语法	IA5String
multi- 或 Single-Valued	多值
定义在	RFC 2307

8.154. NSACCESSLOG

此条目标识供服务器使用的访问日志。

OID	nsAccessLog-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.155. NSADMINACCESSADDRESSES

此属性包含实例使用的管理服务器的 IP 地址。

OID	nsAdminAccessAddresses-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape 管理服务

8.156. NSADMINACCESSHOSTS

此属性包含管理服务器的主机名。

OID	nsAdminAccessHosts-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape 管理服务

8.157. NSADMINACCOUNTINFO

此属性包含有关管理服务器帐户的其他信息。

OID	nsAdminAccountInfo-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape 管理服务

8.158. NSADMINCACHELIFETIME

这会设定存储目录服务器使用的缓存的时间长度。

OID	nsAdminCacheLifetime-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape 管理服务

8.159. NSADMINCGIWAITPID

此属性定义管理服务器 CGI 进程 ID 的等待时间。

OID	nsAdminCgiWaitPid-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape 管理服务

8.160. NSADMINDOMAINNAME

此属性包含包含 Directory Server 实例的管理域的名称。

OID	nsAdminDomainName-oid

语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape 管理服务

8.161. NSADMINENABLEENDUSER

此属性设定是否允许最终用户访问 admin 服务。

OID	nsAdminEnableEnduser-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape 管理服务

8.162. NSADMINENDUSERHTMLINDEX

此属性设定是否允许最终用户访问 admin 服务的 HTML 索引。

OID	nsAdminEndUserHTMLIndex-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape 管理服务

8.163. NSADMINGROUPNAME

此属性提供 admin 指南的名称。

OID	nsAdminGroupName-oid
语法	DirectoryString
multi- 或 Single-Valued	多值

定义在	Netscape 管理服务

8.164. NSADMINONEACLDIR

此属性提供包含管理服务器的访问控制列表的目录路径。

OID	nsAdminOneACLDir-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape 管理服务

8.165. NSADMINSIEDN

此属性包含管理服务器的 ser 实例条目(SIE)的 DN。

OID	nsAdminSIEDN-oid
语法	DN
multi- 或 Single-Valued	多值
定义在	Netscape 管理服务

8.166. NSADMINUSERS

此属性提供包含管理服务器 admin 用户信息的文件的路径和名称。

OID	nsAdminUsers-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape 管理服务

8.167. NSAIMID

此属性包含用户的 AOL Instant Messaging 用户 ID。

OID	2.16.840.1.113730.3.2.300
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	目录服务器

8.168. NSBASEDN

这包括目录服务器的服务器实例定义条目中使用的基本 DN。

OID	nsBaseDN-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	目录服务器

8.169. NSBINDDN

此属性包含目录服务器 SIE 中定义的绑定 DN。

OID	nsBindDN-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	目录服务器

8.170. NSBINDPASSWORD

此属性包含 nsBindDN 中定义的绑定 DN 使用的密码。

OID	nsBindPassword-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	目录服务器

8.171. NSBUILDNUMBER

这在目录服务器 SIE 中定义服务器实例的构建号。

OID	nsBuildNumber-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.172. NSBUILDSECURITY

这在目录服务器 SIE 中定义构建安全级别。

OID	nsBuildSecurity-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.173. NSCERTCONFIG

此属性定义 Red Hat Certificate System 的配置。

OID	nsCertConfig-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	证书系统

8.174. NSCLASSNAME

OID	nsClassname-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.175. NSCONFIGROOT

此属性包含配置目录的根 DN。

OID	nsConfigRoot-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.176. NSCPAIMSCREENNAME

此属性为用户提供 AIM 屏幕名称。

OID	1.3.6.1.4.1.13769.2.4
语法	TelephoneString
multi- 或 Single-Valued	多值

定义在	Mozilla Address Book

8.177. NSDEFAULTACCEPTLANGUAGE

此属性包含 HTML 客户端接受的语言代码。

OID	nsDefaultAcceptLanguage-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.178. NSDEFAULTOBJECTCLASS

此属性将对象类信息存储在容器条目中。

OID	nsDefaultObjectClass-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape 管理服务

8.179. NSDELETECLASSNAME

OID	nsDeleteclassname-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape 管理服务

8.180. NSDIRECTORYFAILOVERLIST

此属性包含用于故障转移的目录服务器列表。

OID	nsDirectoryFailoverList-oid
语法	IA5String
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.181. NSDIRECTORYINFOREF

此属性引用包含服务器信息的条目的 DN。

OID	nsDirectoryInfoRef-oid
语法	DN
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.182. NSDIRECTORYURL

此属性包含目录服务器 URL。

OID	nsDirectoryURL-oid
语法	IA5String
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.183. NSDISPLAYNAME

此属性包含显示名称。

OID	nsDisplayName-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape 管理服务

8.184. NSERRORLOG

此属性标识服务器使用的错误日志。

OID	nsErrorLog-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.185. NSEXECREF

此属性包含可用于执行服务器任务的可执行文件的路径或位置。

OID	nsExecRef-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.186. NSEXPIRATIONDATE

此属性包含应用程序的过期日期。

OID	nsExpirationDate-oid

语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.187. NSGROUPRDNCOMPONENT

此属性定义用于组条目的 RDN 的属性。

OID	nsGroupRDNComponent-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.188. NSHARDWAREPLATFORM

此属性指示服务器在其上运行的硬件。此属性的值与来自 uname -m 的输出相同。例如：

> ***nsHardwarePlatform:i686***

OID	nsHardwarePlatform-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.189. NSHELPREF

此属性包含对在线帮助文件的引用。

OID	nsHelpRef-oid
语法	DirectoryString

multi- 或 Single-Valued	多值
定义在	RFC 2256

8.190. NSHOSTLOCATION

此属性包含有关服务器主机的信息。

OID	nsHostLocation-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.191. NSICQID

此属性包含用户的 ICQ ID。

OID	2.16.840.1.113730.3.1.2014
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	目录服务器

8.192. NSINSTALLEDLOCATION

此属性包含版本 7.1 或更早版本的目录服务器的安装目录。

OID	nsInstalledLocation-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.193. NSJARFILENAME

此属性提供控制台使用的 jar 文件名称。

OID	nsJarfilename-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.194. NSLDAPSCHEMAVERSION

这提供了 LDAP 目录模式的版本号。

OID	nsLdapSchemaVersion-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.195. NSLICENSEDFOR

nsLicensedFor 属性标识用户要使用的服务器。管理服务器要求每个 nsLicenseUser 条目包含此属性的零个或多个实例。此属性的有效关键字包括：

- *slapd，获得许可的目录服务器客户端。*
- *许可邮件服务器客户端的邮件。*
- *用于 许可的新闻服务器客户端。*
- *cal 用于许可的扩展服务器客户端。*

例如：

> ***nsLicensedFor: slapd***

OID	2.16.840.1.113730.3.1.36
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	管理服务器

8.196. NSLICENSEENDTIME

保留供以后使用。

OID	2.16.840.1.113730.3.1.38
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	管理服务器

8.197. NSLICENSESTARTTIME

保留供以后使用。

OID	2.16.840.1.113730.3.1.37
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	管理服务器

8.198. NSLOGSUPPRESS

此属性设定是否阻止服务器日志记录。

OID	nsLogSuppress-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape

8.199. NSMSGDISALLOWACCESS

此属性定义对消息传递服务器的访问。

OID	nsmsgDisallowAccess-oid
语法	IA5String
multi- 或 Single-Valued	多值
定义在	Netscape Messaging Server

8.200. NSMSGNUMMSGQUOTA

此属性为消息传递服务器要保留的消息数量设置配额。

OID	nsmsgNumMsgQuota-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape Messaging Server

8.201. NSMSNID

此属性包含用户的 MSN 即时消息 ID。

OID	2.16.840.1.113730.3.1.2016
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	目录服务器

8.202. NSNICKNAME

此属性为应用程序提供 nickname。

OID	nsNickName-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape

8.203. NSNYR

OID	nsNYR-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	管理服务

8.204. NSOSVERSION

此属性包含运行服务器的主机的版本号。

OID	nsOsVersion-oid
语法	DirectoryString
multi- 或 Single-Valued	多值

定义在	Netscape

8.205. NSPIDLOG

OID	nsPidLog-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape

8.206. NSPREFERENCE

此属性存储控制台首选项设置。

OID	nsPreference-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape 管理服务

8.207. NSPRODUCTNAME

这包括产品的名称，如 {PRODUCT} 或 Administration Server。

OID	nsProductName-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape

8.208. NSPRODUCTVERSION

这包括目录服务器的版本号。

OID	nsProductVersion-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape

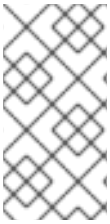
8.209. NSREVISIONNUMBER

此属性包含目录服务器或管理服务器的修订号。

OID	nsRevisionNumber-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape

8.210. NSSECURESERVERPORT

此属性包含 Directory 服务器的 TLS 端口。



注意

此属性不会为 Directory 服务器配置 TLS 端口。这在 Directory 服务器的 dse.ldif 文件中的 nsslapd-secureport 配置属性中配置。配置 、 命令和文件参考 中描述了配置属性。

OID	nsSecureServerPort-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	目录服务器

8.211. NSSERIALNUMBER

此属性包含分配给特定服务器应用程序的序列号或跟踪号，如 {PRODUCT} 或 Administration Server。

OID	nsSerialNumber-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape

8.212. NSSERVERADDRESS

此属性包含运行目录服务器的服务器主机的 IP 地址。

OID	nsServerAddress-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape

8.213. NSSERVERCREATIONCLASSNAME

此属性提供创建服务器时要使用的类名称。

OID	nsServerCreationClassname-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape

8.214. NSSERVERID

它包含服务器的实例名称。例如：

```
nsServerID: slapd-example
```

OID	nsServerID-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape

8.215. NSSERVERMIGRATIONCLASSNAME

此属性包含迁移服务器时要使用的类名称。

OID	nsServerMigrationClassname-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape

8.216. NSSERVERPORT

此属性包含目录服务器的标准 LDAP 端口。

注意

此属性不会为目录服务器 配置 标准端口。这在 Directory 服务器的 dse.ldif 文件中的 nsslapd-port 配置属性中配置。配置 、 命令和文件参考 中描述了配置属性。

OID	nsServerPort-oid
语法	DirectoryString
multi- 或 Single-Valued	多值

定义在	Netscape

8.217. NSSERVERSECURITY

这显示了目录服务器是否需要安全 TLS 或 SSL 连接。

OID	nsServerSecurity-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape

8.218. NSSNMPCONTACT

此属性包含 SNMP 提供的联系信息。

OID	2.16.840.1.113730.3.1.235
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	目录服务器

8.219. NSSNMPDESCRIPTION

这包括 SNMP 服务的描述。

OID	2.16.840.1.113730.3.1.236
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	目录服务器

8.220. NSSNMPENABLED

此属性显示是否为服务器启用了 SNMP。

OID	2.16.840.1.113730.3.1.232
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	目录服务器

8.221. NSSNMPLOCATION

此属性显示 SNMP 服务提供的位置。

OID	2.16.840.1.113730.3.1.234
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	目录服务器

8.222. NSSNMPMASTERHOST

此属性显示 SNMP master 代理的主机名。

OID	2.16.840.1.113730.3.1.237
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	目录服务器

8.223. NSSNMPMASTERPORT

此属性显示 SNMP 子代理的端口号。

OID	2.16.840.1.113730.3.1.238
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	目录服务器

8.224. NSSNMPORGANIZATION

此属性包含 SNMP 提供的机构信息。

OID	2.16.840.1.113730.3.1.233
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	目录服务器

8.225. NSSUITESPOTUSER

此属性已被弃用。

此属性标识安装服务器的 Unix 用户。

OID	nsSuiteSpotUser-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape

8.226. NSTASKLABEL

OID	nsTaskLabel-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape

8.227. NSUNIQUEATTRIBUTE

这会为服务器首选项设置唯一属性。

OID	nsUniqueAttribute-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape 管理服务

8.228. NSUSERIDFORMAT

此属性设置用于从 givenname 和 sn 属性生成 uid 属性的格式。

OID	nsUserIDFormat-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape 管理服务

8.229. NSUSERRDNCOMPONENT

此属性设置属性 type，为用户条目设置 RDN。

OID	nsUserRDNComponent-oid

语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape 管理服务

8.230. NSVALUEBIN

OID	2.16.840.1.113730.3.1.247
语法	二进制
multi- 或 Single-Valued	多值
定义在	Netscape servers - 值项

8.231. NSVALUECES

OID	2.16.840.1.113730.3.1.244
语法	IA5String
multi- 或 Single-Valued	多值
定义在	Netscape servers - 值项

8.232. NSVALUECIS

OID	2.16.840.1.113730.3.1.243
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape servers - 值项

8.233. NSVALUEDEFAULT

OID	2.16.840.1.113730.3.1.250
语法	DirectoryString

multi- 或 Single-Valued	多值
定义在	Netscape servers - 值项

8.234. NSVALUEDESCRIPTION

OID	2.16.840.1.113730.3.1.252
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape servers - 值项

8.235. NSVALUEDN

OID	2.16.840.1.113730.3.1.248
语法	DN
multi- 或 Single-Valued	多值
定义在	Netscape servers - 值项

8.236. NSVALUEFLAGS

OID	2.16.840.1.113730.3.1.251
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape servers - 值项

8.237. NSVALUEHELPURL

OID	2.16.840.1.113730.3.1.254
语法	IA5String
multi- 或 Single-Valued	多值

定义在	Netscape servers - 值项

8.238. NSVALUEINT

OID	2.16.840.1.113730.3.1.246
语法	整数
multi- 或 Single-Valued	多值
定义在	Netscape servers - 值项

8.239. NSVALUESYNTAX

OID	2.16.840.1.113730.3.1.253
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape servers - 值项

8.240. NSVALUETEL

OID	2.16.840.1.113730.3.1.245
语法	TelephoneString
multi- 或 Single-Valued	多值
定义在	Netscape servers - 值项

8.241. NSVALUETYPE

OID	2.16.840.1.113730.3.1.249
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape servers - 值项

8.242. NSVENDOR

这包括服务器厂商的名称。

OID	nsVendor-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape

8.243. NSVIEWCONFIGURATION

此属性存储控制台使用的视图配置。

OID	nsViewConfiguration-oid
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape 管理服务

8.244. NSVIEWFILTER

此属性设置属性-值对，用于识别属于视图的条目。

OID	2.16.840.1.113730.3.1.3023
语法	IA5String
multi- 或 Single-Valued	多值
定义在	目录服务器

8.245. NSWELLKNOWNJARFILES

OID	nsWellKnownJarfiles-oid

语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape 管理服务

8.246. NSWMEXTENDEDUSERPREFS

此属性用于将帐户的用户首选项存储在消息传递服务器中。

OID	2.16.840.1.113730.3.1.520
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape Messaging Server

8.247. NSYIMID

此属性包含用户的 Yahoo instant 消息传递用户名。

OID	2.16.840.1.113730.3.1.2015
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	目录服务器

8.248. NTGROUPATTRIBUTES

此属性指向包含组信息的二进制文件。例如：

```
ntGroupAttributes:: IyEvYmluL2tzaAoKIwojIGRlZmF1bHQgdmFsdWUKIwplPSJgaG9zdG5hb
```

OID	2.16.840.1.113730.3.1.536
语法	二进制

multi- 或 Single-Valued	单值
定义在	Netscape NT 同步

8.249. NTGROUPCREATENEWGROUP

Windows Sync 使用 ntGroupCreateNewGroup 属性来确定 Directory Server 是否应该在 Windows 服务器上创建新组条目。true 创建新条目； false 忽略 Windows 条目。

OID	2.16.840.1.113730.3.1.45
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	Netscape NT 同步

8.250. NTGROUPDELETEGROUP

Windows Sync 使用 ntGroupDeleteGroup 属性来确定 Directory Server 是否应该在 Windows 同步对等服务器上删除组条目。true 表示帐户被删除； false 忽略删除。

OID	2.16.840.1.113730.3.1.46
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	Netscape NT 同步

8.251. NTGROUPDOMAINID

ntGroupDomainID 属性包含组的域 ID 字符串。

> ***ntGroupDomainId: DS HR Group***

OID	2.16.840.1.113730.3.1.44
语法	DirectoryString

multi- 或 Single-Valued	单值
定义在	Netscape NT 同步

8.252. NTGROUPID

ntGroupId 属性指向用于标识组的二进制文件。例如：

```
ntGroupId: lOUnHNjjRgghghREgfvltrGHyuTYhjlOhTYtyHJuSDwOopKLhjGbnGFtr
```

OID	2.16.840.1.113730.3.1.110
语法	二进制
multi- 或 Single-Valued	单值
定义在	Netscape NT 同步

8.253. NTGROUPTYPE

在 Active Directory 中，有两个主要组：安全性和分发。安全组与目录服务器中的组最相似，因为安全组可以配置有针对访问控制、资源限制和其他权限的策略。分布组用于邮件分发。它们进一步划分成全局组和本地组。Directory Server ntGroupType 支持所有四个组类型：

ntGroupType 属性标识 Windows 组的类型。有效值如下：

- *-21483646 用于 global/security*
- *-21483644 用于域 local/security*
- *2 用于全局/发布*
- *4 用于域本地/分发*

当 Windows 组同步时，会自动设置这个值。要确定组类型，您必须在创建组时手动配置它。默认情况

下，Directory Server 组没有此属性，并同步为全局/安全组。

> ***ntGroupType: -21483646***

OID	2.16.840.1.113730.3.1.47
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	Netscape NT 同步

8.254. NTUNIQUEID

ntUniqueId 属性包含为内部服务器识别和操作生成的数字。例如：

> ***ntUniqueId: 352562404224a44ab040df02e4ef500b***

OID	2.16.840.1.113730.3.1.111
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	Netscape NT 同步

8.255. NTUSERACCTEXPIRES

此属性指示条目的 Windows 帐户何时过期。这个值以 GMT 格式存储。例如：

> ***ntUserAcctExpires: 20081015203415***

OID	2.16.840.1.113730.3.1.528
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	Netscape NT 同步

8.256. NTUSERAUTHFLAGS

此属性包含为 Windows 帐户设置的授权标志。

OID	2.16.840.1.113730.3.1.60
语法	二进制
multi- 或 Single-Valued	单值
定义在	Netscape NT 同步

8.257. NTUSERBADPWCOUNT

此属性设置在帐户锁定前允许错误密码失败的数量。

OID	2.16.840.1.113730.3.1.531
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	Netscape NT 同步

8.258. NTUSERCODEPAGE

ntUserCodePage 属性包含用户选择语言的代码页面。例如：

```
ntUserCodePage: AAAAAA==
```

OID	2.16.840.1.113730.3.1.533
语法	二进制
multi- 或 Single-Valued	单值
定义在	Netscape NT 同步

8.259. NTUSERCOMMENT

此属性包含有关用户条目的文本描述或备注。

OID	2.16.840.1.113730.3.1.522
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	Netscape NT 同步

8.260. NTUSERCOUNTRYCODE

此属性包含用户所在国家的双字符国家/地区。

OID	2.16.840.1.113730.3.1.532
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	Netscape NT 同步

8.261. NTUSERCREATENEWACCOUNT

Windows Sync 使用 ntUserCreateNewAccount 属性来确定目录服务器在 Windows 服务器上创建新用户时是否应创建新的用户条目。true 创建新条目； false 忽略 Windows 条目。

OID	2.16.840.1.113730.3.1.42
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	Netscape NT 同步

8.262. NTUSERDELETEACCOUNT

Windows Sync 使用的 ntUserDeleteAccount 属性 IS，以确定当用户从 Windows 同步对等服务器中删除时是否自动删除目录服务器条目。true 表示用户条目被删除； false 忽略删除。

OID	2.16.840.1.113730.3.1.43
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	Netscape NT 同步

8.263. NTUSERDOMAINID

ntUserDomainId 属性包含 Windows 域登录 ID。例如：

```
ntUserDomainId: jsmith
```

OID	2.16.840.1.113730.3.1.41
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	Netscape NT 同步

8.264. NTUSERFLAGS

此属性包含为 Windows 帐户设置的额外标志。

OID	2.16.840.1.113730.3.1.523
语法	二进制
multi- 或 Single-Valued	单值
定义在	Netscape NT 同步

8.265. NTUSERHOMEDIR

ntUserHomeDir 属性包含代表 Windows 用户的主目录的 ASCII 字符串。此属性可以是 null。例如：

```
ntUserHomeDir: c:\jsmith
```

OID	2.16.840.1.113730.3.1.521
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	Netscape NT 同步

8.266. NTUSERHOMEDIRDRIVE

此属性包含有关存储用户主目录的驱动器的信息。

OID	2.16.840.1.113730.3.1.535
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	Netscape NT 同步

8.267. NTUSERLASTLOGOFF

ntUserLastLogoff 属性包含最后一次 logoff 的时间。这个值以 GMT 格式存储。

如果启用了安全日志记录，则只有在用户条目的某些其他方面发生变化时，才会在同步时更新此属性。

> **ntUserLastLogoff: 20201015203415Z**

OID	2.16.840.1.113730.3.1.527
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	Netscape NT 同步

8.268. NTUSERLASTLOGON

ntUserLastLogon 属性包含用户最后一次登录到 Windows 域的时间。这个值以 GMT 格式存储。如果

启用了安全日志记录，则只有在用户条目的某些其他方面发生变化时，才会在同步时更新此属性。

> ***ntUserLastLogon: 20201015203415Z***

OID	2.16.840.1.113730.3.1.526
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	Netscape NT 同步

8.269. NTUSERLOGONHOURS

ntUserLogonHours 属性包含允许用户登录到 Active Directory 域的时间段。此属性对应于 Active Directory 中的 logonHours 属性。

OID	2.16.840.1.113730.3.1.530
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	Netscape NT 同步

8.270. NTUSERLOGONSERVER

ntUserLogonServer 属性定义用户登录请求的 Active Directory 服务器。

OID	2.16.840.1.113730.3.1.65
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	Netscape NT 同步

8.271. NTUSERMAXSTORAGE

ntUserMaxStorage 属性包含用户可用的最大磁盘空间量。

> ***ntUserMaxStorage: 4294967295***

OID	2.16.840.1.113730.3.1.529
语法	二进制
multi- 或 Single-Valued	单值
定义在	Netscape NT 同步

8.272. NTUSERNUMLOGONS

此属性显示用户对 Active Directory 域的成功日志数量。

OID	2.16.840.1.113730.3.1.64
语法	二进制
multi- 或 Single-Valued	单值
定义在	Netscape NT 同步

8.273. NTUSERPARMS

ntUserParms 属性包含保留供应用使用的 Unicode 字符串。

OID	2.16.840.1.113730.3.1.62
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	Netscape NT 同步

8.274. NTUSERPASSWORDEXPIRED

此属性显示 Active Directory 帐户的密码是否已过期。

OID	2.16.840.1.113730.3.1.68
语法	二进制
multi- 或 Single-Valued	单值
定义在	Netscape NT 同步

8.275. NTUSERPRIMARYGROUPID

ntUserPrimaryGroupId 属性包含用户所属的主组的组 ID。

OID	2.16.840.1.113730.3.1.534
语法	二进制
multi- 或 Single-Valued	单值
定义在	Netscape NT 同步

8.276. NTUSERPRIV

此属性显示用户允许的特权类型。

OID	2.16.840.1.113730.3.1.59
语法	二进制
multi- 或 Single-Valued	单值
定义在	Netscape NT 同步

8.277. NTUSERPROFILE

ntUserProfile 属性包含用户配置集的路径。例如：

```
ntUserProfile: c:\jsmith\profile.txt
```

OID	2.16.840.1.113730.3.1.67
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	Netscape NT 同步

8.278. NTUSERSCRIPTPATH

ntUserScriptPath 属性包含用户用来登录到域的 ASCII 脚本的路径。

```
ntUserScriptPath: c:\jstorm\lscript.bat
```

OID	2.16.840.1.113730.3.1.524
语法	二进制
multi- 或 Single-Valued	单值
定义在	Netscape NT 同步

8.279. NTUSERUNIQUEID

ntUserUniqueId 属性包含 Windows 用户的唯一数字 ID。

OID	2.16.840.1.113730.3.1.66
语法	二进制
multi- 或 Single-Valued	单值
定义在	Netscape NT 同步

8.280. NTUSERUNITSPERWEEK

ntUserUnitsPerWeek 属性包含用户登录 Active Directory 域的时间总量。

OID	2.16.840.1.113730.3.1.63
语法	二进制
multi- 或 Single-Valued	单值
定义在	Netscape NT 同步

8.281. NTUSERUSRCOMMENT

ntUserUsrComment 属性包含有关用户的额外注释。

OID	2.16.840.1.113730.3.1.61
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	Netscape NT 同步

8.282. NTUSERWORKSTATIONS

ntUserWorkstations 属性包含允许用户登录的工作站的 ASCII 字符串的名称列表。最多可以列出 8 个工作站，用逗号分开。指定 null 以允许用户从任何工作站登录。例如：

```
ntUserWorkstations: firefly
```

OID	2.16.840.1.113730.3.1.525
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	Netscape NT 同步

8.283. O

organizationName 或 o 属性包含机构名称。例如：

> ***organizationName: Example Corporation***
> ***o: Example Corporation***

OID	2.5.4.10
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.284. OBJECTCLASS

iwl 属性标识用于条目的对象类。例如：

> ***objectClass: person***

OID	2.5.4.0
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.285. OBJECTCLASSES

此属性用于模式文件来识别 subschema 定义所允许的对象类。

OID	2.5.21.6
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2252

8.286. OBSOLETEDBYDOCUMENT

obsoletedByDocument 属性包含已过时的文档条目的可分辨名称。

OID	0.9.2342.19200300.102.1.4
语法	DN
multi- 或 Single-Valued	多值
定义在	Internet White Pages Pilot

8.287. OBSOLETESDOCUMENT

obsoletesDocument 属性包含文档的可分辨名称，这些文档条目已过时。

OID	0.9.2342.19200300.102.1.3
语法	DN
multi- 或 Single-Valued	多值
定义在	Internet White Pages Pilot

8.288. ONCRPCNUMBER

oncRpcNumber 属性包含 RPC 映射的一部分，并存储 UNIX RPC 的 RPC 号。

注意

oncRpcNumber 属性在 Directory Server 中的 10rfc2307.ldif 中定义。要使用更新的 RFC 2307 模式，请删除 10rfc2307.ldif 文件，并将 10rfc2307bis.ldif 文件从 /usr/share/dirsrv/data 目录复制到 /etc/dirsrv/slapd-instance/schema 目录。

OID	1.3.6.1.1.1.1.18
语法	整数
multi- 或 Single-Valued	单值
定义在	RFC 2307

8.289. ORGANIZATIONALSTATUS

organizationalStatus 标识机构中的人员类别。

> *organizationalStatus: researcher*

OID	0.9.2342.19200300.100.1.45
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 1274

8.290. OTHERMAILBOX

otherMailbox 属性包含 X.400 和 RFC 822 以外的电子邮件类型值。

> *otherMailbox: internet $ jsmith@example.com*

OID	0.9.2342.19200300.100.1.22
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 1274

8.291. OU

organizationalUnitName 或 ou，包含组织部门的名称或目录层次结构中的子树。

> *organizationalUnitName: Marketing*
> *ou: Marketing*

OID	2.5.4.11
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.292. OWNER

owner 属性包含负责条目的个人的 DN。例如：

```
owner: cn=John Smith,ou=people,dc=example,dc=com
```

OID	2.5.4.32
语法	DN
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.293. PAGER

pagerTelephoneNumber 或 pager 属性包含个人的 pager 电话号码。

```
pagerTelephoneNumber: 415-555-6789
pager: 415-555-6789
```

OID	0.9.2342.19200300.100.1.42
语法	telephoneNumber
multi- 或 Single-Valued	多值
定义在	RFC 1274

8.294. PARENTORGANIZATION

parentOrganization 属性标识机构或组织单元的父机构。

OID	1.3.6.1.4.1.1466.101.120.41
语法	DN
multi- 或 Single-Valued	单值
定义在	Netscape

8.295. PERSONALSIGNATURE

personalSignature 属性包含条目的签名文件，采用二进制格式。

personalSignature:: AAAAAA==

OID	0.9.2342.19200300.100.1.53
语法	二进制
multi- 或 Single-Valued	多值
定义在	RFC 1274

8.296. PERSONALTITLE

personalTitle 属性包含个人的尊重，如 Ms.、Dr.、Prof. 和 Rev。

personalTitle: Mr.

OID	0.9.2342.19200300.100.1.40
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 1274

8.297. PHOTO

photo 属性包含一个二进制格式的照片文件。

photo:: AAAAAA==

OID	0.9.2342.19200300.100.1.7
语法	二进制
multi- 或 Single-Valued	多值

定义在	RFC 1274

8.298. PHYSICALDELIVERYOFFICENAME

physicalDeliveryOffice 包含物理送送办事处所在的城市或 town。

> ***physicalDeliveryOfficeName: Raleigh***

OID	2.5.4.19
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.299. POSTALADDRESS

postalAddress 属性标识条目的 mailing 地址。此字段旨在包含多个行。当以 LDIF 格式表示时，每行都应用美元符号($)分隔。

要在条目文本中代表实际美元符号($)或反斜杠(\)，请分别使用转义的十六进制值 \24 和 \5c。例如，要代表字符串：

> ***The dollar ($) value can be found***
> ***in the c:\cost file.***

提供字符串：

> ***The dollar (\24) value can be found$in the c:\5ccost file.***

OID	2.5.4.16
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.300. POSTALCODE

postalCode 包含位于美国条目的 zip 代码。

postalCode: 44224

OID	2.5.4.17
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.301. POSTOFFICEBOX

postOfficeBox 属性包含条目物理邮件地址的邮寄地址号或 post office box 号。

postOfficeBox: 1234

OID	2.5.4.18
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.302. PREFERREDDELIVERYMETHOD

preferredDeliveryMethod 包含条目的首选联系人或交付方法。例如：

preferredDeliveryMethod: telephone

OID	2.5.4.28
语法	DirectoryString
multi- 或 Single-Valued	多值

定义在	RFC 2256

8.303. PREFERREDLANGUAGE

preferredLanguage 属性包含个人的首选写入或 spoken 语言。该值应符合 HTTP Accept-Language 标头值的语法。

OID	2.16.840.1.113730.3.1.39
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	RFC 2798

8.304. PREFERREDLOCALE

区域标识了特定区域用户、文化或自定义期望数据的信息，包括如何解释给定语言的数据以及如何对数据进行排序。目录服务器支持美国英语、日语和德语的三个区域。

preferredLocale 属性设定用户首选区域设置。

OID	1.3.6.1.4.1.1466.101.120.42
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	Netscape

8.305. PREFERREDTIMEZONE

preferredTimeZone 属性设置用于用户条目的时区。

OID	1.3.6.1.4.1.1466.101.120.43
语法	DirectoryString

multi- 或 Single-Valued	单值
定义在	Netscape

8.306. PRESENTATIONADDRESS

presentationAddress 属性包含条目的 OSI presentation 地址。此属性包括 OSI 网络地址和最多三个选择器，各自供传输、会话和演示实体使用。例如：

> *presentationAddress: TELEX+00726322+RFC-1006+02+130.59.2.1*

OID	2.5.4.29
语法	IA5String
multi- 或 Single-Valued	单值
定义在	RFC 2256

8.307. PROTOCOLINFORMATION

protocolInformation 属性与 presentationAddress 属性一同使用，提供有关 OSO 网络服务的附加信息。

OID	2.5.4.48
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.308. PWDRESET

当管理员更改用户的密码时，目录服务器会将用户条目中的 pwdReset operational 属性设置为 true。应用可以使用此属性来识别管理员是否重置了用户的密码。

注意

pwdReset 属性是一个操作属性，因此用户无法编辑它。

OID	1.3.6.1.4.1.1466.115.121.1.7
语法	布尔值
multi- 或 Single-Valued	单值
定义在	RFC draft-behera-ldap-password-policy

8.309. REF

ref 属性用于支持 LDAPv3 智能引用。此属性的值是 LDAP URL：

> **ldap: pass:quotes[host_name]:pass:quotes[port_number]/pass:quotes[subtree_dn]**

端口号是可选的。

例如：

> **ref: ldap://server.example.com:389/ou=People,dc=example,dc=com**

OID	2.16.840.1.113730.3.1.34
语法	IA5String
multi- 或 Single-Valued	多值
定义在	LDAPv3 Referrals Internet Draft

8.310. REGISTEREDADDRESS

此属性包含接收电话或加速文档的邮政地址。在交付时，通常需要接收者的签名。

OID	2.5.4.26

语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.311. ROLEOCCUPANT

此属性包含 organizationalRole 条目中定义的角色中操作的可分辨名称。

> ***roleOccupant: uid=bjensen,dc=example,dc=com***

OID	2.5.4.33
语法	DN
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.312. ROOMNUMBER

此属性指定对象的空间号。cn 属性应该用于命名房间对象。

> ***roomNumber: 230***

OID	0.9.2342.19200300.100.1.6
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 1274

8.313. SEARCHGUIDE

searchGuide 属性指定在目录树中将条目用作搜索操作的基本对象时建议搜索条件的信息。在构建搜索过滤器时，请使用 enhancedSearchGuide 属性。

OID	2.5.4.14
语法	IA5String
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.314. SECRETARY

secretary 属性标识条目的 secretary 或 administrative assistant。

> ***secretary: cn=John Smith,dc=example,dc=com***

OID	0.9.2342.19200300.100.1.21
语法	DN
multi- 或 Single-Valued	多值
定义在	RFC 1274

8.315. SEEALSO

seeAlso 属性标识可能包含与这个条目相关的信息的另外一个 Directory Server 条目。

> ***seeAlso: cn=Quality Control Inspectors,ou=manufacturing,dc=example,dc=com***

OID	2.5.4.34
语法	DN
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.316. SERIALNUMBER

serialNumber 属性包含设备的序列号。

> ***serialNumber: 555-1234-AZ***

OID	2.5.4.5
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.317. SERVERHOSTNAME

serverHostName 属性包含运行目录服务器的服务器的主机名。

OID	2.16.840.1.113730.3.1.76
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	红帽管理服务

8.318. SERVERPRODUCTNAME

serverProductName 属性包含服务器产品的名称。

OID	2.16.840.1.113730.3.1.71
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	红帽管理服务

8.319. SERVERROOT

此属性已过时。

此属性显示 Directory Servers 版本 7.1 或更早版本的安装目录（服务器根）。

OID	2.16.840.1.113730.3.1.70
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape 管理服务

8.320. SERVERVERSIONNUMBER

serverVersionNumber 属性包含服务器版本号。

OID	2.16.840.1.113730.3.1.72
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	红帽管理服务

8.321. SHADOWEXPIRE

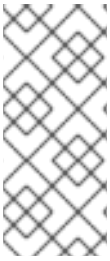
shadowExpire 属性包含 shadow 帐户过期的日期。日期的格式是 EPOCH (UTC)起的天数。要计算在系统上，请运行以下命令，使用 -d 作为当前日期，使用 -u 指定 UTC：

```
$ echo date -u -d 20100108 +%s /24/60/60 |bc

14617
```

其结果（示例中为 14617），然后是 shadowExpire 的值。

```
shadowExpire: 14617
```



注意

shadowExpire 属性在目录服务器中的 10rfc2307.ldif 中定义。要使用更新的 RFC 2307 模式，请删除 10rfc2307.ldif 文件，并将 10rfc2307bis.ldif 文件从 /usr/share/dirsrv/data 目录复制到 /etc/dirsrv/slapd-instance/schema 目录。

OID	1.3.6.1.1.1.1.10
语法	整数
multi- 或 Single-Valued	单值
定义在	RFC 2307

8.322. SHADOWFLAG

shadowFlag 属性标识影子映射中的哪些区域存储标志值。

```
shadowFlag: 150
```

注意

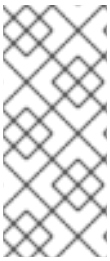
shadowFlag 属性在目录服务器中的 10rfc2307.ldif 中定义。要使用更新的 RFC 2307 模式，请删除 10rfc2307.ldif 文件，并将 10rfc2307bis.ldif 文件从 /usr/share/dirsrv/data 目录复制到 /etc/dirsrv/slapd-instance/schema 目录。

OID	1.3.6.1.1.1.1.11
语法	整数
multi- 或 Single-Valued	单值
定义在	RFC 2307

8.323. SHADOWINACTIVE

shadowInactive 属性设置影子帐户可以不活跃的时间（以天为单位）。

```
shadowInactive: 15
```



注意

shadowInactive 属性在目录服务器中的 10rfc2307.ldif 中定义。要使用更新的 RFC 2307 模式，请删除 10rfc2307.ldif 文件，并将 10rfc2307bis.ldif 文件从 /usr/share/dirsrv/data 目录复制到 /etc/dirsrv/slapd-instance/schema 目录。

OID	1.3.6.1.1.1.1.9
语法	整数
multi- 或 Single-Valued	单值
定义在	RFC 2307

8.324. SHADOWLASTCHANGE

shadowLastChange 属性包含 1970 年 1 月 1 日和上次设置用户密码的天数。例如，如果在 2016 年 11 月 4 日上设置了帐户密码，shadowLastChange 属性将设置为 0

以下例外是存在的：

- *当在 cn=config 条目中启用 passwordMustChange 参数时，新帐户在 shadowLastChange 属性中设置 0。*
- *当您创建没有密码的帐户时，不会添加 shadowLastChange 属性。*

shadowLastChange 属性会自动为从 Active Directory 同步的帐户更新。

注意

shadowLastChange 属性在 Directory Server 中的 10rfc2307.ldif 中定义。要使用更新的 RFC 2307 模式，请删除 10rfc2307.ldif 文件，并将 10rfc2307bis.ldif 文件从 /usr/share/dirsrv/data 目录复制到 /etc/dirsrv/slapd-instance/schema 目录。

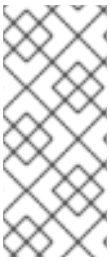
OID	1.3.6.1.1.1.1.5

语法	整数
multi- 或 Single-Valued	单值
定义在	RFC 2307

8.325. SHADOWMAX

shadowMax 属性设置影子密码有效的最大天数。

```
shadowMax: 10
```



注意

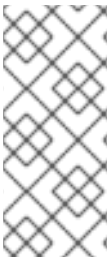
shadowMax 属性在目录服务器中的 10rfc2307.ldif 中定义。要使用更新的 RFC 2307 模式，请删除 10rfc2307.ldif 文件，并将 10rfc2307bis.ldif 文件从 /usr/share/dirsrv/data 目录复制到 /etc/dirsrv/slapd-instance/schema 目录。

OID	1.3.6.1.1.1.1.7
语法	整数
multi- 或 Single-Valued	单值
定义在	RFC 2307

8.326. SHADOWMIN

shadowMin 属性设置在更改影子密码之间必须传递的最小天数。

```
shadowMin: 3
```



注意

shadowMin 属性在目录服务器中的 10rfc2307.ldif 中定义。要使用更新的 RFC 2307 模式，请删除 10rfc2307.ldif 文件，并将 10rfc2307bis.ldif 文件从 /usr/share/dirsrv/data 目录复制到 /etc/dirsrv/slapd-instance/schema 目录。

OID	1.3.6.1.1.1.1.6
语法	整数
multi- 或 Single-Valued	单值
定义在	RFC 2307

8.327. SHADOWWARNING

shadowWarning 属性设定密码过期前几天，向用户发送警告。

shadowWarning: 2

注意

shadowWarning 属性在目录服务器中的 10rfc2307.ldif 中定义。要使用更新的 RFC 2307 模式，请删除 10rfc2307.ldif 文件，并将 10rfc2307bis.ldif 文件从 /usr/share/dirsrv/data 目录复制到 /etc/dirsrv/slapd-instance/schema 目录。

OID	1.3.6.1.1.1.1.8
语法	整数
multi- 或 Single-Valued	单值
定义在	RFC 2307

8.328. SINGLELEVELQUALITY

singleLevelQuality 在目录树的下立即指定分配的数据质量。

OID	0.9.2342.19200300.100.1.50
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	RFC 1274

8.329. SN

surname 或 sn, 属性包含一个条目的 surname， 也称为姓氏或系列名称。

```
surname: Jensen
sn: Jensen
```

OID	2.5.4.4
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.330. ST

stateOrProvinceName 或 st， 属性包含条目的 state 或 province。

```
stateOrProvinceName: California
st: California
```

OID	2.5.4.8
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.331. STREET

streetAddress 或 street, 属性包含条目的 street name 和 residential 地址。

```
streetAddress: 1234 Ridgeway Drive
street: 1234 Ridgeway Drive
```

OID	2.5.4.9
语法	DirectoryString

multi- 或 Single-Valued	多值
定义在	RFC 2256

8.332. SUBJECT

subject 属性包含有关文档条目的主题问题的信息。

> ***subject: employee option grants***

OID	0.9.2342.19200300.102.1.8
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Internet White Pages Pilot

8.333. SUBTREEMAXIMUMQUALITY

subtreeMaximumQuality 属性指定目录子树的最大数据质量。

OID	0.9.2342.19200300.100.1.52
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	RFC 1274

8.334. SUBTREEMINIMUMQUALITY

subtreeMinimumQuality 指定目录子树的最小数据质量。

OID	0.9.2342.19200300.100.1.51
语法	DirectoryString
multi- 或 Single-Valued	单值

定义在	RFC 1274

8.335. SUPPORTEDALGORITHMS

supportedAlgorithms 属性包含请求并存储在二进制格式的算法，如 supportedAlgorithms;binary。

> ***supportedAlgorithms:: AAAAAA==***

OID	2.5.4.52
语法	二进制
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.336. SUPPORTEDAPPLICATIONCONTEXT

此属性包含 OSI 应用上下文的标识符。

OID	2.5.4.30
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.337. TELEPHONENUMBER

telephoneNumber 包含条目的电话号码。例如：

> ***telephoneNumber: 415-555-2233***

OID	2.5.4.20
语法	telephoneNumber

multi- 或 Single-Valued	多值
定义在	RFC 2256

8.338. TELETEXTERMINALIDENTIFIER

teletexTerminalIdentifier 属性包含条目的 teletex 终端标识符。示例中的第一个可打印字符串是要编码的 teletex 终端标识符的第一个部分编码，后续的 0 或更多字节字符串是 teletex 终端标识符的后续部分：

```
teletex-id = ttx-term 0*("$" ttx-param)
ttx-term = printablestring
ttx-param = ttx-key ":" ttx-value
ttx-key = "graphic" / "control" / "misc" / "page" / "private"
ttx-value = octetstring
```

OID	2.5.4.22
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.339. TELEXNUMBER

此属性定义条目的 telex 号。telex 号的格式如下：

```
actual-number "$" country "$" answerback
```

- *实际数字是 要编码的电话数部分的语法形式。*
- *国家/地区 是 TELEX 国家/地区代码。*
- *answerback 是 TELEX 终端的回答代码。*

OID	2.5.4.21

语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.340. TITLE

title 属性包含机构中的人员标题。

> ***title: Senior QC Inspector***

OID	2.5.4.12
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.341. TTL

TimeToLive、或 ttl 属性包含缓存条目信息的时间（以秒为单位）。过指定时间后，信息将被视为过期。值为零(0)表示不应缓存该条目。

> ***TimeToLive: 120***
> ***ttl: 120***

OID	1.3.6.1.4.250.1.60
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	LDAP 缓存互联网生成

8.342. UID

userID 更常见的 uid 属性包含条目的唯一用户名。

```
userID: jsmith
uid: jsmith
```

OID	0.9.2342.19200300.100.1.1
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 1274

8.343. UIDNUMBER

uidNumber 属性包含用户条目的唯一标识符。这与 Unix 中的用户号类似。

```
uidNumber: 120
```

注意

uidNumber 属性在目录服务器中的 10rfc2307.ldif 中定义。要使用更新的 RFC 2307 模式，请删除 10rfc2307.ldif 文件，并将 10rfc2307bis.ldif 文件从 /usr/share/dirsrv/data 目录复制到 /etc/dirsrv/slapd-instance/schema 目录。

OID	1.3.6.1.1.1.1.0
语法	整数
multi- 或 Single-Valued	单值
定义在	RFC 2307

8.344. UNIQUEIDENTIFIER

此属性标识了一个特定项，用于在可分辨名称被重复使用时区分两个条目。此属性旨在检测对已删除的可分辨名称的引用实例。此属性由服务器分配。

```
uniqueIdentifier:: AAAAAA==
```

OID	0.9.2342.19200300.100.1.44

语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 1274

8.345. UNIQUEMEMBER

uniqueMember 属性标识与一个条目关联的一组名称，其中每个名称被赋予一个 uniqueIdentifier 以确保其唯一性。uniqueMember 属性的值是一个 DN，后跟 uniqueIdentifier。

OID	2.5.4.50
语法	DN
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.346. UPDATEDBYDOCUMENT

updatedByDocument 属性包含文档的可分辨名称，这是文档条目的更新版本。

OID	0.9.2342.19200300.102.1.6
语法	DN
multi- 或 Single-Valued	多值
定义在	Internet White Pages Pilot

8.347. UPDATESDOCUMENT

updatesDocument 属性包含本文档是一个更新版本的文档的可分辨名称。

OID	0.9.2342.19200300.102.1.5
语法	DN

multi- 或 Single-Valued	多值
定义在	Internet White Pages Pilot

8.348. USERCERTIFICATE

此属性以二进制形式存储和请求，格式为 userCertificate;binary。

```
userCertificate;binary:: AAAAAA==
```

OID	2.5.4.36
语法	二进制
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.349. USERCLASS

此属性指定计算机用户的类别。此属性的语义是任意的。organizationalStatus 属性与计算机用户和其他类型的用户之间没有区别，且可能更为适用。

```
userClass: intern
```

OID	0.9.2342.19200300.100.1.8
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 1274

8.350. USERPASSWORD

此属性以 {encryption method} 加密密码格式标识条目的密码和加密方法。例如：

```
userPassword: {sha}FTSLQhxXpA05
```

强烈建议不要传输明文密码，其中底层传输服务无法保证保密性。传输明文可能会导致密码被暴露给未经授权的方。

OID	2.5.4.35
语法	二进制
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.351. USERPKCS12

此属性为个人身份信息交换提供格式。属性以二进制形式存储和请求，格式为 userPKCS12;binary。属性值是 PFX PDU，存储为二进制数据。

OID	2.16.840.1.113730.3.1.216
语法	二进制
multi- 或 Single-Valued	多值
定义在	RFC 2798

8.352. USERSMIMECERTIFICATE

userSMIMECertificate 属性包含可供邮件客户端用于 S/MIME 的证书。此属性以二进制格式请求并存储数据。例如：

```
userSMIMECertificate;binary:: AAAAAA==
```

OID	2.16.840.1.113730.3.1.40
语法	二进制
multi- 或 Single-Valued	多值
定义在	RFC 2798

8.353. VACATIONENDDATE

此属性显示用户 vacation 周期的结束日期。

OID	2.16.840.1.113730.3.1.708
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape Messaging Server

8.354. VACATIONSTARTDATE

此属性显示用户的 vacation 周期的开始日期。

OID	2.16.840.1.113730.3.1.707
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	Netscape Messaging Server

8.355. X121ADDRESS

x121Address 属性包含用户的 X.121 地址。

OID	2.5.4.24
语法	IA5String
multi- 或 Single-Valued	多值
定义在	RFC 2256

8.356. X500UNIQUEIDENTIFIER

保留供以后使用。X.500 标识符是一种二进制方法，在可分辨名称被重复使用时，对于不同的对象很有用。

x500UniqueIdentifier:: AAAAAA==

OID	2.5.4.45
语法	二进制
multi- 或 Single-Valued	多值
定义在	RFC 2256

第 9 章 条目对象类参考

此引用是默认 schema 接受的对象类的字母顺序列表。它为每个对象类提供定义，并列出其必需属性和允许的属性。列出的对象类可用于支持条目信息。

当该对象类添加到目录的 ldif 文件中时，为对象类列出所需的属性必须存在于条目中。如果对象类具有高级对象类，该条目中必须同时存在这两个带有所有必要属性的对象类。如果没有在 ldif 文件中列出所需的属性，则服务器不会重启。

注意

对象类允许 LDAP RFC 和 X.500 标准具有多个高级对象类。目录服务器目前不支持此行为。

9.1. ACCOUNT

帐户 对象类定义计算机帐户的条目。此对象类在 RFC 1274 中定义。

优越的类

top

OID

0.9.2342.19200300.100.4.5

表 9.1. 必要属性

属性	定义
objectClass	提供条目的对象类。
userID	提供定义的帐户用户 ID。

表 9.2. 允许的属性

属性	定义
description	提供条目的文本描述。

属性	定义
主机	提供帐户所在的机器的主机名。
localityName	提供条目的城市或地理位置。
organizationName	提供帐户所属的机构。
organizationalUnitName	提供帐户所属组织单元或部门。
seeAlso	包含指向另一个条目或站点的 URL，以及相关信息。

9.2. ACCOUNTPOLICY

***accountpolicy** 对象类定义帐户取消激活或过期策略的条目。这用于用户目录配置条目，它与 Account Policy 插件配置结合使用。*

优越的类

top

OID

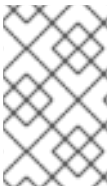
1.3.6.1.4.1.11.1.3.2.2.1

表 9.3. 允许的属性

属性	定义
accountInactivityLimit	在帐户锁定不活跃前，设置帐户最后一次登录时间（以秒为单位）。

9.3. ALIAS

***alias** 对象类指向其他目录条目。此对象类在 RFC 2256 中定义。*



注意

{PRODUCT} 不支持别名条目。

优越的类

top

OID

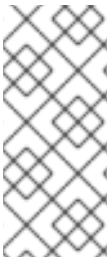
2.5.6.1

表 9.4. 必要属性

属性	定义
objectClass	定义条目的对象类。
aliasedObjectName	给出该条目的可分辨名称。

9.4. BOOTABLEDEVICE

bootableDevice 对象类指向带有引导参数的设备。此对象类在 RFC 2307 中定义。



注意

此对象类在目录服务器中的 10rfc2307.ldif 中定义。要使用更新的 RFC 2307 模式，请删除 10rfc2307.ldif 文件，并将 10rfc2307bis.ldif 文件从 /usr/share/dirsrv/data 目录复制到 /etc/dirsrv/slapd-instance/schema 目录。

优越的类

top

OID

1.3.6.1.1.1.2.12

表 9.5. 必要属性

属性	定义
objectClass	定义条目的对象类。
commonName	提供设备的通用名称。

表 9.6. 允许的属性

属性	定义
bootFile	提供引导镜像文件。
bootParameter	为设备提供引导过程使用的参数。
description	提供条目的文本描述。
localityName	提供条目的城市或地理位置。
organizationName	提供设备所属的机构。
organizationalUnitName	提供设备所属的组织单元或部门。
owner	为负责该设备的人员提供 DN （区分名称）。
seeAlso	包含指向另一个条目或站点的 URL，以及相关信息。
serialNumber	包含设备的序列号。

9.5. CACHEOBJECT

cacheObject 是一个包含生存时间(ttl)属性类型的对象。此对象类在 LDAP 缓存互联网 Draft 中定义。

优越的类

top

OID

1.3.6.1.4.1.250.3.18

表 9.7. 必要属性

属性	定义
objectClass	定义条目的对象类。

表 9.8. 允许的属性

属性	定义
timeToLive	对象保留在缓存中的时间（处于活动状态）。

9.6. COSCLASSICDEFINITION

cosClassicDefinition 对象类使用条目的 DN （区分名称）以及 cosTemplateDn 属性中的其中一个目标属性（在 cosSpecifier 属性中指定的）定义服务模板条目的类。

此对象类在 RFC 1274 中定义。

优越的类

cosSuperDefinition

OID

2.16.840.1.113730.3.2.100

表 9.9. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
cosAttribute	提供 CoS 生成值的属性名称。可以指定多个 **cosAttribute** 值。

表 9.10. 允许的属性

属性	定义
commonName	提供条目的通用名称。
cosSpecifier	指定典型的 CoS 使用的属性值，它以及模板条目的 DN，用于标识模板条目。
cosTemplateDn	提供与 CoS 定义关联的模板条目的 DN。
description	提供条目的文本描述。

9.7. COSDEFINITION

cosDefinition 对象类定义正在使用的服务类；此对象类提供与 DS4.1 CoS 插件的兼容性。

此对象类在 RFC 1274 中定义。

优越的类

top

OID

2.16.840.1.113730.3.2.84

表 9.11. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。

表 9.12. 允许的属性

属性	定义
aci	当 Directory 服务器从客户端收到 LDAP 请求时，评估授予或拒绝哪些权限。
commonName	提供条目的通用名称。
cosAttribute	提供 CoS 生成值的属性名称。可以指定多个 **cosAttribute** 值。
cosSpecifier	指定典型的 CoS 使用的属性值，它以及模板条目的 DN，用于标识模板条目。
cosTargetTree	定义 CoS 模式应用到的目录中的子树。
cosTemplateDn	提供与 CoS 定义关联的模板条目的 DN。
userID	为该条目提供用户 ID。

9.8. COSINDIRECTDEFINITION

cosIndirectDefinition 使用其中一个目标条目属性的值定义模板条目。目标条目的属性在 cosIndirectSpecifier 属性中指定。

此对象类由 Directory Server 定义。

优越的类

cosSuperDefinition

OID

2.16.840.1.113730.3.2.102

表 9.13. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
cosAttribute	提供 CoS 生成值的属性名称。可以指定多个 **cosAttribute** 值。

表 9.14. 允许的属性

属性	定义
commonName	提供条目的通用名称。
cosIndirectSpecifier	指定间接 CoS 用于识别模板条目的属性值。
description	提供条目的文本描述。

9.9. COSPOINTERDEFINITION

此对象类使用模板条目的 DN 值标识与 CoS 定义关联的模板条目。模板条目的 DN 在 cosIndirectSpecifier 属性中指定。

此对象类由 Directory Server 定义。

优越的类

cosSuperDefinition

OID

2.16.840.1.113730.3.2.101

表 9.15. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
cosAttribute	提供 CoS 生成值的属性名称。可以指定多个 **cosAttribute** 值。

表 9.16. 允许的属性

属性	定义
commonName	提供条目的通用名称。
cosTemplateDn	提供与 CoS 定义关联的模板条目的 DN。
description	提供条目的文本描述。

9.10. COSSUPERDEFINITION

所有 CoS 定义对象类从 cosSuperDefinition 对象类继承。

此对象类由 Directory Server 定义。

优越的类

ldapsubentry

OID

2.16.840.1.113730.3.2.99

表 9.17. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
cosAttribute	提供 CoS 生成值的属性名称。可以指定多个 **cosAttribute** 值。

表 9.18. 允许的属性

属性	定义
commonName	提供条目的通用名称。
description	提供条目的文本描述。

9.11. COSTEMPLATE

***cosTemplate** 对象类包含 CoS 的共享属性值列表。*

此对象类由 Directory Server 定义。

优越的类

top

OID

2.16.840.1.113730.3.2.128

表 9.19. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。

表 9.20. 允许的属性

属性	定义
commonName	提供条目的通用名称。

属性	定义
cosPriority	指定当 CoS 模板竞争提供属性值时，哪个模板提供属性值。

9.12. COUNTRY

国家/地区 对象类定义代表国家/地区的条目。此对象类在 RFC 2256 中定义。

优越的类

top

OID

2.5.6.2

表 9.21. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
countryName	在 目录中包含代表国家名称（由 ISO 定义）的双字符代码。

表 9.22. 允许的属性

属性	定义
description	提供条目的文本描述。
searchGuide	在将条目用作搜索的目录树中的基本对象时，指定推荐的搜索条件的信息。

9.13. DCOBJECT

dcObject 对象类允许为条目定义域组件。此对象类定义为辅助性，因为它通常与另一个对象类一起使用，如 o (organization)、 ou (organizationalUnit)或 l (locality)。

例如：

```
dn: dc=example,dc=com
objectClass: top
objectClass: organizationalUnit
objectClass: dcObject
dc: example
ou: Example Corporation
```

此对象类在 RFC 2247 中定义。

优越的类

top

OID

1.3.6.1.4.1.1466.344

表 9.23. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
dc	包含域名的一个组件。

9.14. DEVICE

设备 对象类将网络设备（如打印机）的信息存储在 目录中。此对象类在 RFC 2247 中定义。

优越的类

top

OID

2.5.6.14

表 9.24. 必要属性

属性	定义
objectClass	提供分配给设备的对象类。
commonName	提供设备的通用名称。

表 9.25. 允许的属性

属性	定义
description	提供条目的文本描述。
localityName	提供条目的城市或地理位置。
organizationName	提供设备所属的机构。
organizationalUnitName	提供设备所属的组织单元或部门。
owner	为负责该设备的人员提供 DN （区分名称）。
seeAlso	包含指向另一个条目或站点的 URL，以及相关信息。
serialNumber	包含设备的序列号。

9.15. 文档

文档对象类定义代表文档的 目录条目。RFC 1247.

优越的类

top

OID

0.9.2342.19200300.100.4.6

表 9.26. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
documentIdentifier	提供文档的唯一 ID。

表 9.27. 允许的属性

属性	定义
abstract	包含文档摘要。
audio	以二进制格式存储声音文件。
authorCn	给出作者的通用名称或指定名称。
authorSn	给出作者姓氏。
commonName	提供条目的通用名称。
description	提供条目的文本描述。
dITRedirect	包含条目的 DN （区分名称），用作文档条目的重定向。
documentAuthor	包含作者的 DN （区分名称）。
documentLocation	提供原始文档的位置。
documentPublisher	标识发布该文档的人员或组织。
documentStore	
documentTitle	包含文档的标题。
documentVersion	提供文档的版本号。
info	包含有关文档的信息。
jpegPhoto	存储 JPG 镜像。
keyWords	包含与文档相关的关键字。
localityName	提供条目的城市或地理位置。
lastModifiedBy	提供修改文档条目的最后一个用户的 DN （区分名称）。
lastModifiedTime	提供最后一次修改的时间。
Manager	提供条目管理器的 DN （区分名称）。
organizationName	提供文档所属的机构。

属性	定义
obsoletedByDocument	为其他文档条目的 DN （区分名称）提供过期本文档的另一文档条目。
obsoletesDocument	*为另一文档条目提供 DN （区分名称），该条目已由*本文档过时。
organizationalUnitName	提供文档所属组织单元或部门。
photo	以二进制格式存储文档的照片。
seeAlso	包含指向另一个条目或站点的 URL，以及相关信息。
subject	描述文档的主题。
uniqueIdentifier	当可分辨名称被重复使用时，可以区分两个条目。
updatedByDocument	为 *更新* 本文档的其他文档条目提供 DN （区分名称）。
updatesDocument	提供本文档 *更新* 的另一文档条目的 DN （区分名称）。

9.16. DOCUMENTSERIES

***documentSeries** 对象类定义一个代表一系列文档的条目。此对象类在 RFC 1274 中定义。*

优越的类

top

OID

0.9.2342.19200300.100.4.9

表 9.28. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
commonName	提供条目的通用名称。

表 9.29. 允许的属性

属性	定义
description	提供条目的文本描述。
localityName	提供文档系列物理位置。
organizationName	提供文档系列所属的机构。
organizationalUnitName	提供系列所属的组织单元或部门。
seeAlso	包含指向另一个条目或站点的 URL，以及相关信息。
telephoneNumber	提供负责文档系列的人员的电话号码。

9.17. DOMAIN

域 对象类定义代表 DNS 域的目录条目。使用 dc 属性命名此对象类的条目。

此对象类也用于互联网域名，如 example.com。

域 对象类只能用于与机构、机构单元或为其定义了对象类的任何其他对象的目录条目。定义对象类的对象。

此对象类在 RFC 2252 中定义。

优越的类

top

OID

0.9.2342.19200300.100.4.13

表 9.30. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。

属性	定义
dc	包含域名的一个组件。

表 9.31. 允许的属性

属性	定义
associatedName	指定与 DNS 域关联的组织目录树中的条目名称。
businessCategory	给出这个域参与的商业类型。
description	提供条目的文本描述。
destinationIndicator	提供与该条目关联的国家和城市；这一旦需要提供公共电话服务。
facsimileTelephoneNumber	提供域的 fax 号。
internationalISDNNumber	提供域的 ISDN 号。
localityName	提供条目的城市或地理位置。
organizationName	提供条目所属的机构。
physicalDeliveryOfficeName	提供可以进行物理分发的位置。
postOfficeBox	提供域的 post office box 号码。
postalAddress	包含域的电子邮件地址。
postalCode	提供域的邮政代码，如美国的 zip 代码。
preferredDeliveryMethod	显示人员的首选联系方式或消息发送。
General_Atttribute_registeredAddress	当接收者必须验证交付时，提供适合接收快速文档的邮政地址。
searchGuide	在将条目用作搜索的目录树中的基本对象时，指定推荐的搜索条件的信息。
seeAlso	包含指向另一个条目或站点的 URL，以及相关信息。
stateOrProvinceName	提供域所在的状态或省去。
streetaddress	为域物理位置指定 street 名称和地址号。

属性	定义
telephoneNumber	提供域的电话号码。
teletexTerminalIdentifier	提供域的 teletex 终端的 ID。
telexNumber	为域指定电话号。
userPassword	存储条目可以绑定到目录的密码。
x121Address	为域提供 X.121 地址。

9.18. DOMAINRELATEDOBJECT

***domainRelatedObject** 对象类定义代表 DNS 或 NRS 域的条目，它们相当于 X.500 域，如机构或机构单元。*

此对象类在 RFC 1274 中定义。

优越的类

top

OID

0.9.2342.19200300.100.4.17

表 9.32. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
associatedDomain	指定与目录树中的对象关联的 DNS 域。

9.19. DSA

***dSA** 对象类定义代表 DSAs 的条目。*

此对象类在 RFC 1274 中定义。

优越的类

top

OID

2.5.6.13

表 9.33. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
commonName	提供条目的通用名称。
presentationAddress	包含条目的 OSI 演示地址。

表 9.34. 允许的属性

属性	定义
description	提供条目的文本描述。
knowledgeinformation	
localityName	提供条目的城市或地理位置。
organizationName	提供条目所属的机构。
organizationalUnitName	提供条目所属组织单元或部门。
seeAlso	包含指向另一个条目或站点的 URL，以及相关信息。
supportedApplicationContext	包含 OSI 应用上下文的标识符。

9.20. EXTENSIBLEOBJECT

当条目中存在时，scalableObject 允许条目存放可选的任何属性。此类允许的属性列表隐式地设置服务器已知的所有属性。

此对象类在 RFC 2252 中定义。

优越的类

top

OID

1.3.6.1.4.1.1466.101.120.111

表 9.35. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。

允许的属性

服务器已知的所有属性。

9.21. FRIENDLYCOUNTRY

friendlyCountry 对象类定义目录中的国家条目。此对象类允许比 国家 对象类更友好的名称。

此对象类在 RFC 1274 中定义。

优越的类

top

OID

0.9.2342.19200300.100.4.18

表 9.36. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。

属性	定义
friendlyCountryName	存储人类可读的国家/地区名称。
countryName	在 目录中包含代表国家名称（由 ISO 定义）的双字符代码。

表 9.37. 允许的属性

属性	定义
description	提供条目的文本描述。
searchGuide	在将条目用作搜索的目录树中的基本对象时，指定推荐的搜索条件的信息。

9.22. GROUPOFCERTIFICATES

groupOfCertificates 对象类描述了一组 X.509 证书。任何与 memberCertificateDescription 值匹配的证书都被视为组的成员。

优越的类

top

OID

2.16.840.1.113730.3.2.31

表 9.38. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
commonName	提供条目的通用名称。

表 9.39. 允许的属性

属性	定义
businessCategory	提供该组参与的商业类型。

属性	定义
description	提供条目的文本描述。
memberCertificateDescription	包含用于确定特定证书是否为此组的成员的值。
organizationName	提供条目所属的机构。
organizationalUnitName	提供条目所属组织单元或部门。
owner	包含负责组的个人的 DN （区分名称）。
seeAlso	包含指向另一个条目或站点的 URL，以及相关信息。

9.23. GROUPOFMAILENHANCEDUNIQUENAMES

groupOfMailEnhancedUniqueNames 对象类用于必须有唯一成员的邮件组。此对象类是为 Netscape Messaging Server 定义的。

优越的类

top

OID

2.16.840.1.113730.3.2.5

表 9.40. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
commonName	提供条目的通用名称。

表 9.41. 允许的属性

属性	定义
businessCategory	提供该组参与的商业类型。
description	提供条目的文本描述。

属性	定义
mailEnhancedUniqueMember	包含唯一 DN 值来标识邮件组的成员。
organizationName	提供条目所属的机构。
organizationalUnitName	提供条目所属组织单元或部门。
owner	包含负责组的个人的 DN （区分名称）。
seeAlso	包含指向另一个条目或站点的 URL，以及相关信息。

9.24. GROUPOFNAMES

***groupOfNames** 对象类包含一组名称的条目。此对象类在 RFC 2256 中定义。*

注意

Directory 服务器中的此对象类的定义与标准定义不同。在标准定义中，member 是必需属性，而 Directory Server 中则是一个允许的属性。因此，目录服务器允许组没有成员。

优越的类

top

OID

2.5.6.9

表 9.42. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
commonName	提供条目的通用名称。

表 9.43. 允许的属性

属性	定义
businessCategory	给出了条目参与的商业类型。
description	提供条目的文本描述。
成员	包含组成员的 DN （区分名称）。
organizationName	提供条目所属的机构。
organizationalUnitName	提供条目所属组织单元或部门。
owner	包含负责组的个人的 DN （区分名称）。
seeAlso	包含指向另一个条目或站点的 URL，以及相关信息。

9.25. GROUPOFUNIQUENAMES

***groupOfUniqueNames** 对象类定义一个包含唯一名称的组。*

注意

Directory 服务器中的此对象类的定义与标准定义不同。在标准定义中，uniqueMember 是一个必需的属性，而 Directory Server 中是一个允许的属性。因此，目录服务器允许组没有成员。

此对象类在 RFC 2256 中定义。

优越的类

top

OID

2.5.6.17

表 9.44. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
commonName	提供条目的通用名称。

表 9.45. 允许的属性

属性	定义
businessCategory	给出了条目参与的商业类型。
description	提供条目的文本描述。
organizationName	提供条目所属的机构。
organizationalUnitName	提供条目所属组织单元或部门。
owner	包含负责组的个人的 DN （区分名称）。
seeAlso	包含指向另一个条目或站点的 URL，以及相关信息。
uniqueMember	包含组成员的 DN （区分名称）；此 DN 必须是唯一的。

9.26. GROUPOFURLS

groupOfURLs 对象类是 groupOfUniqueNames 和 groupOfNames 对象类的辅助对象类。这个组由标记的 URL 列表组成。

优越的类

top

OID

2.16.840.1.113730.3.2.33

表 9.46. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。

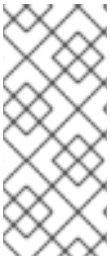
属性	定义
commonName	提供条目的通用名称。

表 9.47. 允许的属性

属性	定义
businessCategory	提供该组参与的商业类型。
description	提供条目的文本描述。
memberURL	包含与组的每个成员关联的 URL。
organizationName	提供条目所属的机构。
organizationalUnitName	提供条目所属组织单元或部门。
owner	包含负责组的个人的 DN （区分名称）。
seeAlso	包含指向另一个条目或站点的 URL，以及相关信息。

9.27. IEEE802DEVICE

***ieee802Device** 对象类指向 MAC 地址的设备。此对象类在 **RFC 2307** 中定义。*



注意

此对象类在目录服务器中的 10rfc2307.ldif 中定义。要使用更新的 RFC 2307 模式，请删除 10rfc2307.ldif 文件，并将 10rfc2307bis.ldif 文件从 /usr/share/dirsrv/data 目录复制到 /etc/dirsrv/slapd-instance/schema 目录。

优越的类

top

OID

1.3.6.1.1.1.2.11

表 9.48. 必要属性

属性	定义
objectClass	定义条目的对象类。
commonName	提供设备的通用名称。

表 9.49. 允许的属性

属性	定义
description	提供条目的文本描述。
localityName	提供条目的城市或地理位置。
macAddress	提供设备的 MAC 地址。
organizationName	提供设备所属的机构。
organizationalUnitName	提供设备所属的组织单元或部门。
owner	为负责该设备的人员提供 DN （区分名称）。
seeAlso	包含指向另一个条目或站点的 URL，以及相关信息。
serialNumber	包含设备的序列号。

9.28. INETADMIN

inetAdmin 对象类是管理组或用户的标记。此对象类是为 Netscape 委派的管理员定义的。

优越的类

top

OID

2.16.840.1.113730.3.2.112

表 9.50. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。

表 9.51. 允许的属性

属性	定义
adminRole	标识管理用户所属的角色。
memberOf	包含管理用户所属的组名称。这由 MemberOf 插件动态管理。

9.29. INETDOMAIN

inetDomain 对象类是虚拟域节点的辅助类。此对象类是为 Netscape 委派的管理员定义的。

优越的类

top

OID

2.16.840.1.113730.3.2.129

表 9.52. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。

表 9.53. 允许的属性

属性	定义
inetDomainBaseDN	定义 DNS 域的用户子树的基本 DN。
inetDomainStatus	提供域的状态。状态可以是 active、active 或 deleted。

9.30. INETORGPERSON

inetOrgPerson 对象类定义代表机构企业网络中人员的条目。此对象类从 person 对象类继承 commonName 和 surname 属性。

此对象类在 RFC 2798 中定义。

优越的类

个人

OID

2.16.840.1.113730.3.2.2

表 9.54. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
commonName	提供条目的通用名称。
surname	提供个人的系列名称或姓氏。

表 9.55. 允许的属性

属性	定义
audio	以二进制格式存储声音文件。
businessCategory	给出了条目参与的商业类型。
carLicense	提供个人载体的许可证号。
departmentNumber	为个人工作的部门提供。
description	提供条目的文本描述。
destinationIndicator	提供与该条目关联的国家和城市；这一旦需要提供公共电话服务。
displayName	显示显示条目时要使用的个人的首选名称。
employeeNumber	包含人员的员工编号。
employeeType	显示个人的雇佣类型（例如，满时）。
facsimileTelephoneNumber	包含个人的传真号。

属性	定义
givenName	包含个人的名字。
homeTelephoneNumber	提供个人的主页电话号码。
homePostalAddress	提供个人的家地址。
初始	给个人的首字母.
internationalISDNNumber	包含条目的 ISDN 号。
jpegPhoto	存储 JPG 镜像。
localityName	提供条目的城市或地理位置。
labeledURI	包含与条目相关的 URL。
mail	包含个人的电子邮件地址。
Manager	包含 person 条目的直接监管器的 DN （区分名称）。
手机	提供个人的手机号码。
organizationName	提供条目所属的机构。
organizationalUnitName	提供条目所属组织单元或部门。
pagerTelephoneNumber	提供个人的页页号。
photo	以二进制格式存储个人的照片。
physicalDeliveryOfficeName	提供可以进行物理分发的位置。
postOfficeBox	提供条目的 post office box 号码。
postalAddress	包含条目的电子邮件地址。
postalCode	提供条目的邮政代码，如美国的 zip 代码。
preferredDeliveryMethod	显示人员的首选联系方式或消息发送。
preferredLanguage	给出个人首选的写入或 spoken 语言。
General_Atttribute_registeredAddress	当接收者必须验证交付时，提供适合接收快速文档的邮政地址。

属性	定义
roomNumber	提供个人所在的房间号。
secretary	包含个人机密或管理助手的 DN （区分名称）。
seeAlso	包含指向另一个条目或站点的 URL，以及相关信息。
stateOrProvinceName	提供条目所在的状态或省去。
streetaddress	为人的物理位置指定 street 名称和编号。
telephoneNumber	提供条目的电话号码。
teletexTerminalIdentifier	提供个人的 teletex 终端的标识符。
telexNumber	提供与条目关联的电话号。
title	显示个人的工作标题。
userID	包含个人的用户 ID （通常是其登录 ID）。
userCertificate	将用户的证书存储在明文中（不使用）。
userPassword	存储条目可以绑定到目录的密码。
userSMIMECertificate	将个人的证书存储为二进制形式，以便 S/MIME 客户端可以使用证书。
x121Address	为个人提供 X.121 地址。
x500UniqueIdentifier	保留供以后使用。

9.31. INETSUBSCRIBER

inetSubscriber 对象类用于常规用户帐户管理。此对象类是为 Netscape 订阅者互操作性定义的。

优越的类

top

OID

2.16.840.1.113730.3.2.134

表 9.56. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。

表 9.57. 允许的属性

属性	定义
inetSubscriberAccountId	包含唯一属性，将订阅者链接到计费系统。
inetSubscriberChallenge	包含某种问题或提示，即用于确认用户身份的质询短语。
inetSubscriberResponse	包含对挑战问题的回答。

9.32. INETUSER

inetUser 对象类是一个辅助类，它必须存在于条目中才能提供订阅者服务。此对象类是为 Netscape 订阅者互操作性定义的。

优越的类

top

OID

2.16.840.1.113730.3.2.130

表 9.58. 必要属性

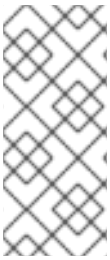
属性	定义
objectClass	提供分配给条目的对象类。

表 9.59. 允许的属性

属性	定义
inetUserHttpURL	包含与用户关联的 Web 地址。
inetUserStatus	授予用户状态。状态可以是 active、active 或 deleted。
memberOf	包含用户所属的组名称。这由 MemberOf 插件动态管理。
userID	包含个人的用户 ID （通常是其登录 ID）。
userPassword	存储用户可用于访问用户帐户的密码。

9.33. IPHOST

***ipHost** 对象类存储主机的 IP 信息。此对象类在 RFC 2307 中定义。*



注意

此对象类在目录服务器中的 10rfc2307.ldif 中定义。要使用更新的 RFC 2307 模式，请删除 10rfc2307.ldif 文件，并将 10rfc2307bis.ldif 文件从 /usr/share/dirsrv/data 目录复制到 /etc/dirsrv/slapd-instance/schema 目录。

优越的类

top

OID

1.3.6.1.1.1.2.6

表 9.60. 必要属性

属性	定义
objectClass	定义条目的对象类。
commonName	提供设备的通用名称。
ipHostNumber	包含设备或主机的 IP 地址。

表 9.61. 允许的属性

属性	定义
description	提供条目的文本描述。
localityName	提供条目的城市或地理位置。
Manager	包含条目的 maintainer 或 supervisor 的 DN （区分名称）。
organizationName	提供设备所属的机构。
organizationalUnitName	提供设备所属的组织单元或部门。
owner	为负责该设备的人员提供 DN （区分名称）。
seeAlso	包含指向另一个条目或站点的 URL，以及相关信息。
serialNumber	包含设备的序列号。

9.34. IPNETWORK

ipNetwork 对象类存储有关网络的 IP 信息。此对象类在 RFC 2307 中定义。

注意

此对象类在目录服务器中的 10rfc2307.ldif 中定义。要使用更新的 RFC 2307 模式，请删除 10rfc2307.ldif 文件，并将 10rfc2307bis.ldif 文件从 /usr/share/dirsrv/data 目录复制到 /etc/dirsrv/slapd-instance/schema 目录。

优越的类

top

OID

1.3.6.1.1.1.2.7

表 9.62. 必要属性

属性	定义
objectClass	定义条目的对象类。
commonName	提供设备的通用名称。
ipNetworkNumber	包含网络的 IP 号。

表 9.63. 允许的属性

属性	定义
description	提供条目的文本描述。
localityName	提供条目的城市或地理位置。
Manager	包含条目的 maintainer 或 supervisor 的 DN （区分名称）。
ipNetmaskNumber	包含网络的 IP 子网掩码。

9.35. IPPROTOCOL

***ipProtocol** 对象类显示 IP 协议版本。此对象类在 RFC 2307 中定义。*

注意

此对象类在目录服务器中的 10rfc2307.ldif 中定义。要使用更新的 RFC 2307 模式，请删除 10rfc2307.ldif 文件，并将 10rfc2307bis.ldif 文件从 /usr/share/dirsrv/data 目录复制到 /etc/dirsrv/slapd-instance/schema 目录。

优越的类

top

OID

1.3.6.1.1.1.2.4

表 9.64. 必要属性

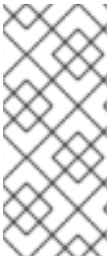
属性	定义
objectClass	定义条目的对象类。
commonName	提供设备的通用名称。
ipProtocolNumber	包含网络的 IP 协议号。

表 9.65. 允许的属性

属性	定义
description	提供条目的文本描述。

9.36. IPSERVICE

***ipService** 对象类存储有关 IP 服务的信息。此对象类在 RFC 2307 中定义。*



注意

此对象类在目录服务器中的 10rfc2307.ldif 中定义。要使用更新的 RFC 2307 模式，请删除 10rfc2307.ldif 文件，并将 10rfc2307bis.ldif 文件从 /usr/share/dirsrv/data 目录复制到 /etc/dirsrv/slapd-instance/schema 目录。

优越的类

top

OID

1.3.6.1.1.1.2.3

表 9.66. 必要属性

属性	定义
objectClass	定义条目的对象类。
commonName	提供设备的通用名称。
ipServicePort	提供 IP 服务使用的端口号。

属性	定义
ipServiceProtocol	包含服务的 IP 协议号。

表 9.67. 允许的属性

属性	定义
description	提供条目的文本描述。

9.37. LABELEDURIOBJECT

此对象类可以添加到现有目录对象中，以允许包含 URI 值。使用此对象类不会根据需要在其他对象类中直接包含 taggedURI 属性类型。

此对象类在 RFC 2079 中定义。

优越的类

top

OID

1.3.6.1.4.1.250.3.15

表 9.68. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。

表 9.69. 允许的属性

属性	定义
labeledURI	提供一个与条目对象相关的 URI。

9.38. 地点

Locality 对象类定义代表本地或地理区域的条目。

此对象类在 RFC 2256 中定义。

优越的类

top

OID

2.5.6.3

表 9.70. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。

表 9.71. 允许的属性

属性	定义
description	提供条目的文本描述。
localityName	提供条目的城市或地理位置。
searchGuide	在将条目用作搜索的目录树中的基本对象时，指定推荐的搜索条件的信息。
seeAlso	包含指向另一个条目或站点的 URL，以及相关信息。
stateOrProvinceName	给出与本地性相关的状态或省。
streetaddress	提供与本地性关联的 street 和数字。

9.39. MAILGROUP

mailGroup 对象类定义组的邮件属性。此对象在 Netscape Messaging Server 的 schema 中定义。

优越的类

top

OID

2.16.840.1.113730.3.2.4

表 9.72. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。

表 9.73. 允许的属性

属性	定义
commonName	提供条目的通用名称。
mail	存储组的电子邮件地址。
mailAlternateAddress	包含组的辅助电子邮件地址。
mailHost	包含邮件服务器的主机名。
owner	包含负责组的个人的 DN （区分名称）。

9.40. MAILRECIPIENT

mailRecipient 对象类为用户定义 mail 帐户。此对象在 Netscape Messaging Server 的 schema 中定义。

优越的类

top

OID

2.16.840.1.113730.3.2.3

表 9.74. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。

表 9.75. 允许的属性

属性	定义
commonName	提供条目的通用名称。
mail	存储组的电子邮件地址。
mailAccessDomain	包含用户可以访问消息传递服务器的域。
mailAlternateAddress	包含组的辅助电子邮件地址。
mailAutoReplyMode	指定是否启用帐户的自动回复模式。
mailAutoReplyText	包含用于自动回复电子邮件的文本。
mailDeliveryOption	指定用于邮件用户的邮件发送机制。
mailForwardingAddress	指定用于邮件用户的邮件发送机制。
mailHost	包含邮件服务器的主机名。
mailMessageStore	指定用户邮件框的位置。
mailProgramDeliveryInfo	指定用于编程邮件发送的命令。
mailQuota	指定用户邮件框允许的磁盘空间。
mailRoutingAddress	包含在将邮件从此条目帐户转发到另一个消息传递服务器时使用的路由地址。
multiLineDescription	包含条目的文本描述，该条目跨越一行。
userID	提供定义的帐户用户 ID。
userPassword	存储条目可以访问该帐户的密码。

9.41. MEPMANAGEDENTRY

mepManagedEntry 对象类标识一个条目，该条目由 Managed Entries 插件的实例生成。此对象类在 Directory Server 中定义。

优越的类

top

OID

2.16.840.1.113730.3.2.319

表 9.76. 允许的属性

属性	定义
mepManagedBy	提供与受管条目对应的原始条目的 DN。

9.42. MEPORIGINENTRY

mepOriginEntry 对象类标识一个条目，该条目由 Managed Entries 插件 的实例 监控，并且具有由插件创建的受管条目，这是原始条目。此对象类在 Directory Server 中定义。

优越的类

top

OID

2.16.840.1.113730.3.2.320

表 9.77. 允许的属性

属性	定义
mepManagedEntry	提供由 Managed Entries 插件实例创建的受管条目的 DN，对应于此原始条目。

9.43. MEPTEMPLATEENTRY

mepTemplateEntry 对象类标识一个条目，该条目由 Managed Entries 插件的实例用作模板，以创建受管条目。此对象类在 Directory Server 中定义。

优越的类

top

OID

2.16.840.1.113730.3.2.321

表 9.78. 允许的属性

属性	定义
commonName	提供条目的通用名称。
mepMappedAttr	包含一个 attribute-token 对，插件用来在受管条目中创建一个属性，其值取自原始条目。
mepRDNAttr	指定在受管条目中用作 naming 属性的属性。
mepStaticAttr	包含在受管条目中将使用的属性值的属性值对。

9.44. NETSCAPECERTIFICATESERVER

netscapeCertificateServer 对象类存储有关 Netscape 证书服务器的信息。此对象在 Netscape 证书管理系统的 schema 中定义。

优越的类

top

OID

2.16.840.1.113730.3.2.18

表 9.79. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。

9.45. NETSCAPEDIRECTORYSERVER

netscapeDirectoryServer 对象类存储有关目录服务器实例的信息。此对象在 Netscape Directory 服

务器的 schema 中定义。

优越的类

top

OID

2.16.840.1.113730.3.2.23

表 9.80. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。

9.46. NETSCAPELINKEDORGANIZATION

NetscapeLinkedOrganization 是一个辅助对象类。此对象在 Netscape 服务器套件的 schema 中定义。

优越的类

top

OID

1.3.6.1.4.1.1466.101.120.141

表 9.81. 允许的属性

属性	定义
parentOrganization	标识为服务器套件定义的链接组织的父机构。

9.47. NETSCAPEMACHINEDATA

netscapeMachineData 对象类区分机器数据和非机器数据。此对象在 Netscape Directory 服务器的 schema 中定义。

优越的类

top

OID

2.16.840.1.113730.3.2.32

9.48. NETSCAPEPREFERENCES

NetscapePreferences 是辅助对象类，用于存储用户首选项。此对象由 Netscape 定义。

优越的类

top

OID

1.3.6.1.4.1.1466.101.120.142

表 9.82. 必要属性

属性	定义
preferredLanguage	给出个人首选的写入或 spoken 语言。
preferredLocale	为个人提供首选区域设置。locale 设置定义 cultural 或 national 设置，如日期格式和货币。
preferredTimeZone	提供个人的首选时区。

9.49. NETSCAPEREVERSIBLEPASSWORDOBJECT

netscapeReversiblePasswordObject 是用于存储密码的辅助对象类。此对象在 Netscape Web 服务器的 schema 中定义。

优越的类

top

OID

2.16.840.1.113730.3.2.154

表 9.83. 允许的属性

属性	定义
netscapeReversiblePassword	包含用于 HTTP Digest/MD5 身份验证的密码。

9.50. NETSCAPESERVER

netscapeServer 对象类包含有关 Netscape 服务器及其安装的实例特定信息。

优越的类

top

OID

2.16.840.1.113730.3.2.10

表 9.84. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
commonName	提供条目的通用名称。

表 9.85. 允许的属性

属性	定义
administratorContactInfo	包含服务器管理员的联系信息。
adminUrl	包含供实例使用的管理服务器的 URL。
description	提供条目的文本描述。
installationTimeStamp	包含服务器实例安装的时间。
serverHostName	包含运行 Directory Server 实例的服务器的主机名。

属性	定义
serverProductName	包含服务器类型的产品名称。
serverRoot	指定安装服务器产品的顶级目录。
serverVersionNumber	包含产品版本号。
userPassword	存储条目可以绑定到目录的密码。

9.51. NETSCAPEWEBSERVER

netscapeWebServer 对象类标识已安装的 Netscape Web Server。

优越的类

top

OID

2.16.840.1.113730.3.2.29

表 9.86. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
commonName	提供条目的通用名称。
nsServerID	包含服务器的名称或 ID。

表 9.87. 允许的属性

属性	定义
description	提供条目的文本描述。
nsServerPort	包含服务器的端口号。

9.52. NEWPILOTPERSON

newPilotPerson 对象类是个人的子类，允许将其他属性分配给 person 对象类的条目。此对象类从 person 对象类继承 commonName 和 surname 属性。

此对象类在 Internet White Pages Pilot 中定义。

优越的类

个人

OID

0.9.2342.19200300.100.4.4

表 9.88. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
commonName	提供条目的通用名称。
surname	提供个人的系列名称或姓氏。

表 9.89. 允许的属性

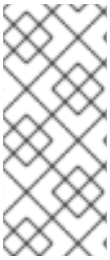
属性	定义
businessCategory	给出了条目参与的商业类型。
description	提供条目的文本描述。
favoriteDrink	为个人提供最喜欢的 drink。
homeTelephoneNumber	提供个人的主页电话号码。
homePostalAddress	提供个人的家地址。
janetMailbox	提供个人的电子邮件地址；这主要用于 Great Britain 或不使用 RFC 8822 邮件地址的组织。
mail	包含个人的电子邮件地址。
mailPreferenceOption	指明用户首选项在邮件列表(electronic 或 physical)中包含其名称。

属性	定义
手机	提供个人的手机号码。
organizationalStatus	为个人的功能提供常见作业类别。
otherMailbox	包含 X.400 和 RFC822 以外的电子邮箱类型的值。
pagerTelephoneNumber	提供个人的页页号。
Personal_Signature_personalSignature	包含个人的签名文件。
personalTitle	给予个人认可。
preferredDeliveryMethod	显示人员的首选联系方式或消息发送。
roomNumber	提供个人所在的房间号。
secretary	包含个人机密或管理助手的 DN （区分名称）。
seeAlso	包含指向另一个条目或站点的 URL，以及相关信息。
telephoneNumber	提供条目的电话号码。
userID	包含个人的用户 ID （通常是其登录 ID）。
userClass	描述此条目的计算机用户的类型。
userPassword	存储条目可以绑定到目录的密码。

9.53. NISMAP

这个对象类指向 NIS 映射。

此对象类在 RFC 2307 中定义，它定义了将 LDAP 用作网络信息服务的对象类和属性。



注意

此对象类在目录服务器中的 10rfc2307.ldif 中定义。要使用更新的 RFC 2307 模式，请删除 10rfc2307.ldif 文件，并将 10rfc2307bis.ldif 文件从 /usr/share/dirsrv/data 目录复制到 /etc/dirsrv/slapd-instance/schema 目录。

优越的类

top

OID

1.3.6.1.1.1.2.13

表 9.90. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
nisMapName	包含 NIS 映射名称。

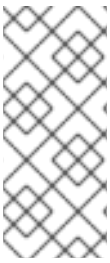
表 9.91. 允许的属性

属性	定义
description	提供条目的文本描述。

9.54. NISNETGROUP

此对象类包含 NIS 域中使用的 netgroup。添加此对象类可让管理员使用网络组来控制 NIS 中的登录和服务身份验证。

此对象类在 RFC 2307 中定义，它定义了将 LDAP 用作网络信息服务的对象类和属性。



注意

此对象类在目录服务器中的 10rfc2307.ldif 中定义。要使用更新的 RFC 2307 模式，请删除 10rfc2307.ldif 文件，并将 10rfc2307bis.ldif 文件从 /usr/share/dirsrv/data 目录复制到 /etc/dirsrv/slapd-instance/schema 目录。

优越的类

top

OID

1.3.6.1.1.1.2.8

表 9.92. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
commonName	提供条目的通用名称。

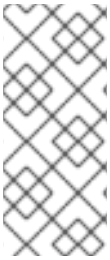
表 9.93. 允许的属性

属性	定义
description	提供条目的文本描述。
memberNisNetgroup	通过列出合并 netgroup 的名称，将另一个 netgroup 的属性值合并到当前组中。
nisNetgroupTriple	包含用户名(、**bobby**、**example.com**)或计算机名称(**shellserver1**、**example.com**)。

9.55. NISOBJECT

此对象类包含有关 NIS 域中对象的信息。

此对象类在 RFC 2307 中定义，它定义了将 LDAP 用作网络信息服务的对象类和属性。



注意

此对象类在目录服务器中的 10rfc2307.ldif 中定义。要使用更新的 RFC 2307 模式，请删除 10rfc2307.ldif 文件，并将 10rfc2307bis.ldif 文件从 /usr/share/dirsrv/data 目录复制到 /etc/dirsrv/slapd-instance/schema 目录。

优越的类

top

OID

1.3.6.1.1.1.2.10

表 9.94. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
commonName	提供条目的通用名称。
NisMapEntry	确定 NIS 映射条目。
nisMapName	包含 NIS 映射的名称。

表 9.95. 允许的属性

属性	定义
description	提供条目的文本描述。

9.56. NSADMINCONFIG

此对象类存储管理服务器的配置参数。此对象是为管理服务定义的。

优越的类

nsConfig

OID

nsAdminConfig-oid

表 9.96. 允许的属性

属性	定义
nsAdminAccessAddresses	标识管理服务器 IP 地址。
nsAdminAccessHosts	包含管理服务器主机名或管理服务器主机名列表。
nsAdminCacheLifetime	请注意缓存超时时间的长度。

属性	定义
nsAdminCgiWaitPid	包含服务器等待的 CGI 进程的 PID。
nsAdminEnableEnduser	设置是否允许或禁止最终用户访问管理服务器 Web 服务页面。
nsAdminOneACLDir	包含管理服务器的本地 ACL 目录的路径。
nsAdminUsers	指向包含 admin 用户信息的文件。

9.57. NSADMINCONSOLEUSER

此对象类存储管理服务器的配置参数。此对象是为管理服务定义的。

优越的类

top

OID

nsAdminConsoleUser-oid

表 9.97. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
commonName	提供条目的通用名称。

表 9.98. 允许的属性

属性	定义
nsPreference	存储控制台设置的首选信息。

9.58. NSADMINDOMAIN

此对象类存储用户信息来访问管理控制台。此对象是为管理服务定义的。

优越的类

organizationalUnit

OID

nsAdminDomain-oid

表 9.99. 允许的属性

属性	定义
nsAdminDomainName	标识服务器的管理域。

9.59. NSADMINGLOBALPARAMETERS

此对象类存储管理服务器的配置参数。此对象是为管理服务定义的。

优越的类

top

OID

nsAdminGlobalParameters-oid

表 9.100. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
commonName	提供条目的通用名称。

表 9.101. 允许的属性

属性	定义
nsAdminEndUserHTMLIndex	设置是否允许或禁止最终用户访问 HTML 索引页面。
nsNickName	提供应用程序的 nickname。

9.60. NSADMINGROUP

此对象类将管理员用户在 Administration Server 中的组信息存储。此对象是为管理服务定义的。

优越的类

top

OID

nsAdminGroup-oid

表 9.102. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
commonName	提供条目的通用名称。

表 9.103. 允许的属性

属性	定义
description	提供条目的文本描述。
nsAdminGroupName	包含 admin 组的名称。
nsAdminSIEDN	显示管理服务器实例实例的服务器实例条目(SIE)的 DN。
nsConfigRoot	提供管理服务器实例配置目录的完整路径。

9.61. NSADMINOBJECT

此对象类包含有关由管理服务器使用的对象的信息，如任务。此对象是为管理服务定义的。

优越的类

top

OID

nsAdminObject-oid

表 9.104. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
commonName	提供条目的通用名称。

表 9.105. 允许的属性

属性	定义
nsClassname	包含与管理服务器的任务或资源编辑器关联的类名称。
nsJarfilename	提供管理控制台用于访问对象的 JAR 文件的名称。

9.62. NSADMINRESOURCEEDITOREXTENSION

此对象类包含 Console Resource Editor 使用的扩展。此对象是为管理服务定义的。

优越的类

nsAdminObject

OID

nsAdminResourceEditorExtension-oid

表 9.106. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
commonName	提供条目的通用名称。

表 9.107. 允许的属性

属性	定义
nsAdminAccountInfo	包含有关管理服务器帐户的信息。
nsDeleteclassname	包含要删除的类的名称。

9.63. NSADMINSERVER

此对象类定义管理服务器实例。此对象是为管理服务定义的。

优越的类

top

OID

nsAdminServer-oid

表 9.108. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
commonName	提供条目的通用名称。
nsServerID	包含目录服务器 ID，如 **slapd-example**。

表 9.109. 允许的属性

属性	定义
description	提供条目的文本描述。

9.64. NSAIMPRESENCE

nsAIMpresence 是辅助对象类，用于定义 AOL 实例消息传递帐户的状态。此对象是为目录服务器定义的。

优越的类

top

OID

2.16.840.1.113730.3.2.300

表 9.110. 允许的属性

属性	定义
nsAIMid	包含条目的 AIM 用户 ID。
nsAIMStatusGraphic	包含指向图形镜像的指针，该镜像指示 AIM 帐户的状态。
nsAIMStatusText	包含用于指示 AIM 帐户状态的文本。

9.65. NSAPPLICATION

nsApplication 定义应用程序或服务器条目。这由 Netscape 定义。

优越的类

top

OID

nsApplication-oid

表 9.111. 必要属性

属性	定义
objectClass	定义条目的对象类。
commonName	提供条目的通用名称。

表 9.112. 允许的属性

属性	定义
description	提供条目的文本描述。

属性	定义
installationTimeStamp	包含服务器实例安装的时间。
nsBuildNumber	包含服务器实例的构建号。
nsBuildSecurity	包含用于进行构建的安全级别。
nsExpirationDate	包含应用程序许可证过期的日期。
nsInstalledLocation	对于版本 7.1 或更早版本的服务器，显示服务器的安装目录。
nsLdapSchemaVersion	提供 Directory 服务器使用的 LDAP 模式文件版本。
nsNickName	提供应用程序的 nickname。
nsProductName	提供服务器产品的名称。
nsProductVersion	显示服务器产品的版本号。
nsRevisionNumber	包含产品的修订版本号（次版本）。
nsSerialNumber	提供分配给服务器产品的序列号。
nsServerMigrationClassname	提供用于迁移服务器实例的类。
nsServerCreationClassname	提供用于创建服务器实例的类。
nsVendor	包含设计服务器的厂商的名称。

9.66. NSCERTIFICATESERVER

nsCertificateServer 对象类存储有关 Red Hat Certificate System 实例的信息。此对象在证书系统的 schema 中定义。

优越的类

top

OID

nsCertificateServer-oid

表 9.113. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
nsServerID	包含服务器的名称或 ID。

表 9.114. 允许的属性

属性	定义
nsCertConfig	包含 Red Hat Certificate System 实例的配置设置。
nsServerPort	包含服务器的端口号。
serverHostName	包含运行目录服务器实例的服务器的主机名。

9.67. NSCOMPLEXROLEDEFINITION

任何不是简单角色的角色都是根据定义的一个复杂角色。

此对象类由 Directory Server 定义。

优越的类

nsRoleDefinition

OID

2.16.840.1.113730.3.2.95

表 9.115. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。

表 9.116. 允许的属性

属性	定义
commonName	提供条目的通用名称。
description	提供条目的文本描述。

9.68. NSCONTAINER

有些条目没有定义任何特定的实体，但它们在目录树中创建一个定义的空间，作为类似或相关子条目的父条目。这些是 容器条目，它们由 nsContainer 对象类标识。

优越的类

top

OID

2.16.840.1.113730.3.2.104

表 9.117. 必要属性

属性	定义
objectClass	定义条目的对象类。
cn	提供条目的通用名称。

9.69. NSCUSTOMVIEW

nsCustomView 对象类定义有关目录服务器数据自定义视图的信息。

优越的类

nsAdminObject

OID

nsCustomView-oid

表 9.118. 允许的属性

属性	定义
nsDisplayName	包含自定义视图设置配置集的名称。

9.70. NSDEFAULTOBJECTCLASSES

nsDefaultObjectClasses 设置在在该目录中创建特定类型的新对象时要使用的默认对象类。这是为管理服务定义的。

优越的类

top

OID

nsDefaultObjectClasses-oid

表 9.119. 必要属性

属性	定义
objectClass	定义条目的对象类。
commonName	提供设备的通用名称。

表 9.120. 允许的属性

属性	定义
nsDefaultObjectClass	包含默认分配给对象类型的对象类。

9.71. NSDIRECTORYINFO

nsDirectoryInfo 包含有关目录实例的信息。这是为管理服务定义的。

优越的类

top

OID

nsDirectoryInfo-oid

表 9.121. 必要属性

属性	定义
objectClass	定义条目的对象类。
commonName	提供设备的通用名称。

表 9.122. 允许的属性

属性	定义
nsBindDN	包含在其服务器实例条目中为服务器定义的绑定 DN。
nsBindPassword	包含 SIE 中绑定身份的密码。
nsDirectoryFailoverList	包含在 **nsDirectoryURL** 中的实例不可用时用于故障切换支持的其他目录服务器实例的 URL 列表。
nsDirectoryInfoRef	包含对目录中可分辨名称(DN)的引用。
nsDirectoryURL	包含用于访问目录服务器实例的 URL。

9.72. NSDIRECTORYSERVER

nsDirectoryServer 是为 Directory Server 实例的定义对象类。这是为目录服务器定义的。

优越的类

top

OID

nsDirectoryServer-oid

表 9.123. 必要属性

属性	定义
objectClass	定义条目的对象类。

属性	定义
nsServerID	包含服务器的名称或 ID。

表 9.124. 允许的属性

属性	定义
nsBaseDN	包含服务器实例的基本 DN。
nsBindDN	包含在其服务器实例条目中为服务器定义的绑定 DN。
nsBindPassword	包含 SIE 中绑定身份的密码。
nsSecureServerPort	包含服务器的 TLS 端口号。
nsServerPort	包含服务器的端口号。
serverHostName	包含运行 Directory Server 实例的服务器的主机名。

9.73. NSFILTEREDROLEDEFINITION

nsFilteredRoleDefinition 对象类定义了条目如何分配给角色，具体取决于每个条目包含的属性。

此对象类在 Directory Server 中定义。

优越的类

nsComplexRoleDefinition

OID

2.16.840.1.113730.3.2.97

表 9.125. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
nsRoleFilter	指定用于识别过滤角色中的条目的过滤器。

表 9.126. 允许的属性

属性	定义
commonName	提供条目的通用名称。
description	提供条目的文本描述。

9.74. NSGLOBALPARAMETERS

nsGlobalParameters 对象类包含全局首选项设置。

此对象类在 Administrative Services 中定义。

优越的类

top

OID

nsGlobalParameters-oid

表 9.127. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
commonName	提供条目的通用名称。

表 9.128. 允许的属性

属性	定义
nsGroupRDNComponent	定义组条目的 RDN 中使用的默认属性类型。
nsUniqueAttribute	在首选项中定义唯一属性。
nsUserIDFormat	设置用于从 **givenname** 和 **sn** 属性生成用户 ID 的格式。
nsUserRDNComponent	设置属性类型，以用作用户 DN 中的命名组件。

属性	定义
nsNYR	未使用。
nsWellKnownJarfiles	未使用。

9.75. NSHOST

nsHost 对象类存储有关服务器主机的信息。

此对象类在 Administrative Services 中定义。

优越的类

top

OID

nsHost-oid

表 9.129. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
commonName	提供条目的通用名称。

表 9.130. 允许的属性

属性	定义
description	提供条目的文本描述。
localityName	提供条目的城市或地理位置。
nsHardwarePlatform	标识运行目录服务器实例的主机的硬件平台。这与运行 **uname -m** 相同。
nsHostLocation	提供服务器主机的位置。

属性	定义
nsOsVersion	包含服务器主机的操作系统版本。
serverHostName	包含运行 Directory Server 实例的服务器的主机名。

9.76. NSICQPRESENCE

nsICQpresence 是辅助对象类，用于定义 ICQ 消息传递帐户的状态。此对象是为目录服务器定义的。

优越的类

top

OID

2.16.840.1.113730.3.2.301

表 9.131. 允许的属性

属性	定义
nsICQid	包含条目的 ICQ 用户 ID。
nsICQStatusGraphic	包含指向图形镜像的指针，指明 ICQ 帐户的状态。
nsICQStatusText	包含用于指示 ICQ 帐户状态的文本。

9.77. NSLICENSEUSER

nsLicenseUser 对象类跟踪基于每个客户端许可的服务器的许可证。nsLicenseUser 旨在与 inetOrgPerson 对象类一起使用。您可以通过管理服务器的 用户和组 区域管理此对象类的内容。

此对象类在 Administration Server schema 中定义。

优越的类

top

OID

2.16.840.1.113730.3.2.7

表 9.132. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。

表 9.133. 允许的属性

属性	定义
nsLicensedFor	标识用户要使用的服务器。
nsLicenseEndTime	保留供以后使用。
nsLicenseStartTime	保留供以后使用。

9.78. NSMANAGEDROLEDEFINITION

nsManagedRoleDefinition 对象类指定角色的成员分配，以明确枚举的成员列表。

此对象类在 Directory Server 中定义。

优越的类

nsComplexRoleDefinition

OID

2.16.840.1.113730.3.2.96

表 9.134. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。

表 9.135. 允许的属性

属性	定义
commonName	提供条目的通用名称。
description	提供条目的文本描述。

9.79. NSMESSAGINGSERVERUSER

nsICQpresence 是描述消息传递服务器用户的辅助对象类。此对象类是为 Netscape Messaging Server 定义的。

优越的类

top

OID

2.16.840.113730.3.2.37

表 9.136. 必要属性

属性	定义
objectClass	提供条目的对象类。

表 9.137. 允许的属性

属性	定义
commonName	提供条目的通用名称。
mailAccessDomain	包含用户可以访问消息传递服务器的域。
mailAlternateAddress	包含组的辅助电子邮件地址。
mailAutoReplyMode	指定是否启用帐户的自动回复模式。
mailAutoReplyText	包含用于自动回复电子邮件的文本。
mailDeliveryOption	指定用于邮件用户的邮件发送机制。
mailForwardingAddress	指定用于邮件用户的邮件发送机制。

属性	定义
mailMessageStore	指定用户邮件框的位置。
mailProgramDeliveryInfo	指定用于编程邮件发送的命令。
mailQuota	指定用户邮件框允许的磁盘空间。
nsmsgDisallowAccess	设置用户可用的邮件协议的限制。
nsmsgNumMsgQuota	指定用户邮件框允许的消息数。
nswmExtendedUserPrefs	存储用户的扩展首选项。
vacationEndDate	包含 vacation 周期的结束日期。
vacationStartDate	包含 vacation 周期的开始日期。

9.80. NSMSNPRESENCE

nsMSNpresence 是辅助对象类，用于定义 MSN 实例消息传递帐户的状态。此对象是为目录服务器定义的。

优越的类

top

OID

2.16.840.1.113730.3.2.303

表 9.138. 允许的属性

属性	定义
nsMSNid	包含条目的 MSN 用户 ID。

9.81. NSNESTEDROLEDEFINITION

nsNestedRoleDefinition 对象类指定一个或多个任何类型的角色，作为角色中的成员包含。

此对象类在 Directory Server 中定义。

优越的类

nsComplexRoleDefinition

OID

2.16.840.1.113730.3.2.98

表 9.139. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
nsRoleDn	指定分配给条目的角色。

表 9.140. 允许的属性

属性	定义
commonName	提供条目的通用名称。
description	提供条目的文本描述。

9.82. NSRESOURCEREF

nsNestedRoleDefinition 对象类配置资源引用。

此对象类在管理服务中定义。

优越的类

top

OID

nsResourceRef-oid

表 9.141. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
commonName	提供条目的通用名称。

表 9.142. 允许的属性

属性	定义
seeAlso	包含指向另一个条目或站点的 URL，以及相关信息。

9.83. NSROLEDEFINITION

所有角色定义对象类从 nsRoleDefinition 对象类继承。

此对象类由 Directory Server 定义。

优越的类

ldapsubentry

OID

2.16.840.1.113730.3.2.93

表 9.143. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。

表 9.144. 允许的属性

属性	定义
commonName	提供条目的通用名称。
description	提供条目的文本描述。

9.84. NSSIMPLEROLEDEFINITION

包含此对象类的角色称为简单角色，因为它们具有有限的灵活性，从而可以轻松地：

- Enumerate 角色的成员。
- 确定给定条目是否具有特定的角色。
- 枚举给定条目拥有的所有角色。
- 为给定条目分配特定角色。
- 从给定条目中删除特定角色。

此对象类由 Directory Server 定义。

优越的类

nsRoleDefinition

OID

2.16.840.1.113730.3.2.94

表 9.145. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。

表 9.146. 允许的属性

属性	定义
commonName	提供条目的通用名称。

属性	定义
description	提供条目的文本描述。

9.85. NSSNMP

此对象类定义 Directory 服务器使用的 SNMP 插件对象的配置。

此对象类在 Directory Server 中定义。

优越的类

top

OID

2.16.840.1.113730.3.2.41

表 9.147. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
commonName	提供条目的通用名称。
nsSNMPEnabled	设置为 Directory 服务器实例启用了 SNMP。

表 9.148. 允许的属性

属性	定义
nsSNMPContact	包含 SNMP 代理提供的联系信息。
nsSNMPDescription	包含 SNMP 设置的文本描述。
nsSNMPLocation	包含 SNMP 代理的位置信息或配置。
nsSNMPMasterHost	包含 SNMP master 代理所在的服务器的主机名。
nsSNMPMasterPort	包含用于访问 SNMP 子代理的端口。

属性	定义
nsSNMPOrganization	包含 SNMP 服务提供的组织名称或信息。

9.86. NSTASK

此对象类定义 Directory 服务器执行的任务配置。

此对象类是为 Administrative Services 定义的。

优越的类

top

OID

nsTask-oid

表 9.149. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
commonName	提供条目的通用名称。

表 9.150. 允许的属性

属性	定义
nsExecRef	包含对将执行任务的程序的引用。
nsHelpRef	包含对与任务窗口关联的在线(HTML)帮助文件的引用。
nsLogSuppress	设置是否阻止任务的日志记录。
nsTaskLabel	包含与控制台中任务关联的标签。

9.87. NSTASKGROUP

此对象类定义控制台中一组任务的信息。

此对象类是为 Administrative Services 定义的。

优越的类

top

OID

nsTaskGroup-oid

表 9.151. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
commonName	提供条目的通用名称。

表 9.152. 允许的属性

属性	定义
nsTaskLabel	包含与控制台中任务关联的标签。

9.88. NSTOPOLOGYCUSTOMVIEW

此对象类配置用于控制台中配置文件的拓扑视图。

此对象类是为 Administrative Services 定义的。

优越的类

nsCustomView

OID

nsTopologyCustomView-oid

表 9.153. 必要属性

属性	定义
commonName	提供条目的通用名称。

表 9.154. 允许的属性

属性	定义
nsViewConfiguration	包含在控制台中使用的视图配置。

9.89. NSTOPOLOGYPLUGIN

此对象类配置用于在控制台中设置视图的拓扑插件。

此对象类是为 Administrative Services 定义的。

优越的类

nsAdminObject

OID

nsTopologyPlugin-oid

9.90. NSVALUEITEM

此对象类定义一个值项对象配置，用于指定依赖于条目值类型的信息。value 项与条目属性的允许属性值语法相关，如二进制或区分大小写的字符串。

此对象类在 Netscape Servers - Value Item 中定义。

优越的类

top

OID

2.16.840.1.113730.3.2.45

表 9.155. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
commonName	提供条目的通用名称。

表 9.156. 允许的属性

属性	定义
nsValueBin	包含与二进制值类型相关的信息或操作。
nsValueCES	包含与 case-exact 字符串(CES)值类型相关的信息或操作。
nsValueCIS	包含与区分大小写(CIS)值类型相关的信息或操作。
nsValueDefault	设置用于属性或配置参数的默认值类型。
nsValueDescription	给出 value 项设置的文本描述。
nsValueDN	包含与 DN 值类型相关的信息或操作。
nsValueFlags	为 value 项对象设置标志。
nsValueHelpURL	包含对与值 item 对象关联的在线(HTML)帮助文件的引用。
nsValueInt	包含与整数值类型相关的信息或操作。
nsValueSyntax	定义用于 value 项对象的语法。
nsValueTel	包含与 telephone string 值类型相关的信息或操作。
nsValueType	设置要应用的值类型。

9.91. NSVIEW

此对象类用于目录树中的视图条目。

此对象类在 Directory Server 中定义。

优越的类

top

OID

2.16.840.1.113730.3.2.304

表 9.157. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
commonName	提供条目的通用名称。

表 9.158. 允许的属性

属性	定义
description	提供条目的文本描述。
nsViewFilter	标识 view 插件使用的过滤器。

9.92. NSYIMPRESENCE

nsYIMpresence 是辅助对象类，用于定义 Yahoo 实例消息传递帐户的状态。此对象是为目录服务器定义的。

优越的类

top

OID

2.16.840.1.113730.3.2.302

表 9.159. 允许的属性

属性	定义
nsYIMid	包含条目的 Yahoo 用户 ID。
nsYIMStatusGraphic	包含指向图形镜像的指针，该镜像指示 Yahoo 帐户的状态。
nsYIMStatusText	包含用于指示 Yahoo 帐户状态的文本。

9.93. NTGROUP

ntGroup 对象类包含存储在 Windows Active Directory 服务器中的组条目的数据。多个目录服务器属性直接对应或映射到 Windows 组属性。当您在 Directory Server 中创建要与 Windows 服务器组同步的新组时，目录服务器属性将分配给 Windows 条目。然后，可以通过目录服务在条目中添加、修改或删除这些属性。

此对象类在 Netscape NT Synchronization 中定义。

优越的类

top

OID

2.16.840.1.113730.3.2.9

表 9.160. 所需的对象类

对象类	定义
mailGroup	允许在 Windows 和 Directory Server 组之间同步 **mail** 属性。

表 9.161. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。

属性	定义
ntUserDomainId	包含组帐户的 Windows 域登录 ID。

表 9.162. 允许的属性

属性	定义
commonName	提供条目的通用名称；这与 Windows **name** 字段对应。
description	提供条目的文本描述；对应于 Windows **注释** 字段。
localityName	提供条目的城市或地理位置。
成员	指定组的成员。
ntGroupCreateNewGroup	指定在 Directory Server 中创建条目时是否应创建 Windows 帐户。
ntGroupDeleteGroup	指定在 Directory Server 中删除条目时是否应该删除 Windows 帐户。
ntGroupDomainId	为组提供域 ID 字符串。
ntGroupType	定义条目所在 Windows 域组的类型。
ntUniqueId	包含服务器用于操作和识别生成的 ID 号。
organizationalUnitName	提供条目所属组织单元或部门。
seeAlso	包含指向另一个条目或站点的 URL，以及相关信息。

9.94. NTUSER

ntUser 条目包含存储在 Windows Active Directory 服务器中的用户条目的数据。多个目录服务器属性直接对应或映射到 Windows 用户帐户字段。当您在 Directory Server 中创建要与 Windows 服务器同步的新 person 条目时，目录服务器属性将分配给 Windows 用户帐户字段。然后，可以通过目录服务在条目中添加、修改或删除这些属性。

此对象类在 Netscape NT Synchronization 中定义。

优越的类

top

OID

2.16.840.1.113730.3.2.8

表 9.163. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
commonName	提供条目的通用名称；这与 Windows **name** 字段对应。
ntUserDomainId	包含用户帐户的 Windows 域登录 ID。

表 9.164. 允许的属性

属性	定义
description	提供条目的文本描述；对应于 Windows **注释** 字段。
destinationIndicator	提供与该条目关联的国家和城市；这一旦需要提供公共电话服务。
facsimileTelephoneNumber	为用户提供传真号。
givenName	包含个人的名字。
homeTelephoneNumber	提供个人的主页电话号码。
homePostalAddress	提供个人的家地址。
初始	给个人的首字母.
localityName	提供条目的城市或地理位置。
mail	包含个人的电子邮件地址。
Manager	包含 person 条目的直接监管器的 DN （区分名称）。
手机	提供个人的手机号码。
ntUserAcctExpires	标识用户的 Windows 帐户何时过期。

属性	定义
ntUserCodePage	为用户提供代码页面。
ntUserCreateNewAccount	指定在 Directory Server 中创建此条目时是否应创建 Windows 帐户。
ntUserDeleteAccount	指定在 Directory Server 中删除此条目时是否应该删除 Windows 帐户。
ntUserHomeDir	提供用户主目录的路径。
ntUserLastLogoff	提供用户从 Windows 服务器进行最后一次登录的时间。
ntUserLastLogon	为用户提供上一次登录 Windows 服务器的时间。
ntUserMaxStorage	显示 Windows 服务器中用户的最大磁盘空间。
ntUserParms	包含保留供应用程序使用的 Unicode 字符串。
ntUserProfile	包含用户 Windows 配置集的路径。
ntUserScriptPath	包含用户 Windows 登录脚本的路径。
ntUserWorkstations	包含允许用户登录 Windows 域的 Windows 工作站列表。
organizationName	提供条目所属的机构。
organizationalUnitName	提供条目所属组织单元或部门。
pagerTelephoneNumber	提供个人的页页号。
postalAddress	包含条目的电子邮件地址。
postalCode	提供条目的邮政代码，如美国的 zip 代码。
postOfficeBox	提供条目的 post office box 号码。
General_Atttribute_registeredAddress	当接收者必须验证交付时，提供适合接收快速文档的邮政地址。
seeAlso	包含指向另一个条目或站点的 URL，以及相关信息。
surname	提供个人的系列名称或姓氏。

属性	定义
stateOrProvinceName	给出个人所在的状态或省去。
streetaddress	为人的物理位置指定 street 名称和地址号。
telephoneNumber	提供条目的电话号码。
teletexTerminalIdentifier	提供个人的 teletex 终端的标识符。
telexNumber	提供与条目关联的电话号。
title	显示个人的工作标题。
userCertificate	将用户的证书存储在明文中（不使用）。
x121Address	为条目提供 X.121 地址。

9.95. ONCRPC

***oncRpc** 对象类定义开放网络计算远程过程调用(ONC RPC)的抽象。此对象类在 RFC 2307 中定义。*

注意

此对象类在目录服务器中的 10rfc2307.ldif 中定义。要使用更新的 RFC 2307 模式，请删除 10rfc2307.ldif 文件，并将 10rfc2307bis.ldif 文件从 /usr/share/dirsrv/data 目录复制到 /etc/dirsrv/slapd-instance/schema 目录。

优越的类

top

OID

1.3.6.1.1.1.2.5

表 9.165. 必要属性

属性	定义
objectClass	定义条目的对象类。

属性	定义
commonName	提供条目的通用名称。
oncRpcNumber	包含 RPC 映射的一部分，并存储 UNIX RPC 的 RPC 号。

表 9.166. 允许的属性

属性	定义
description	提供条目的文本描述。

9.96. 机构

组织属性定义代表机构的条目。通常，组织被认为是大型公司或企业内的大型、相对静态的分组。

此对象类在 RFC 2256 中定义。

优越的类

top

OID

2.5.6.4

表 9.167. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
organizationName	提供条目所属的机构。

表 9.168. 允许的属性

属性	定义
businessCategory	给出了条目参与的商业类型。

属性	定义
description	提供条目的文本描述。
destinationIndicator	提供与该条目关联的国家和城市；这一旦需要提供公共电话服务。
facsimileTelephoneNumber	包含条目的 fax 号。
internationalISDNNumber	包含条目的 ISDN 号。
localityName	提供条目的城市或地理位置。
physicalDeliveryOfficeName	提供可以进行物理分发的位置。
postalAddress	包含条目的电子邮件地址。
postalCode	提供条目的邮政代码，如美国的 zip 代码。
postOfficeBox	提供条目的 post office box 号码。
preferredDeliveryMethod	显示条目的联系人或消息发送的首选方法。
General_Atttribute_registeredAddress	当接收者必须验证交付时，提供适合接收快速文档的邮政地址。
searchGuide	在将条目用作搜索的目录树中的基本对象时，指定推荐的搜索条件的信息。
seeAlso	包含指向另一个条目或站点的 URL，以及相关信息。
stateOrProvinceName	给出个人所在的状态或省去。
streetaddress	为人的物理位置指定 street 名称和编号。
telephoneNumber	提供负责机构的人的电话号码。
teletexTerminalIdentifier	提供条目的 teletex 终端的 ID。
telexNumber	提供与条目关联的电话号。
userPassword	提供条目可以绑定到目录的密码。
x121Address	为条目提供 X.121 地址。

9.97. ORGANIZATIONALPERSON

organizationalPerson 对象类定义了被雇用或附属于机构的人员的条目。此对象类从 person 对象类继承 commonName 和 surname 属性。

此对象类在 RFC 2256 中定义。

优越的类

个人

OID

2.5.6.7

表 9.169. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
commonName	提供条目的通用名称。
surname	提供个人的系列名称或姓氏。

表 9.170. 允许的属性

属性	定义
description	提供条目的文本描述。
destinationIndicator	提供与该条目关联的国家和城市；这一旦需要提供公共电话服务。
facsimileTelephoneNumber	包含条目的 fax 号。
internationalISDNNumber	包含条目的 ISDN 号。
localityName	提供条目的城市或地理位置。
organizationalUnitName	提供条目所属组织单元或部门。
physicalDeliveryOfficeName	提供可以进行物理分发的位置。
postalAddress	包含条目的电子邮件地址。

属性	定义
postalCode	提供条目的邮政代码，如美国的 zip 代码。
postOfficeBox	提供条目的 post office box 号码。
preferredDeliveryMethod	显示人员的首选联系方式或消息发送。
General_Atttribute_registeredAddress	当接收者必须验证交付时，提供适合接收快速文档的邮政地址。
seeAlso	包含指向另一个条目或站点的 URL，以及相关信息。
stateOrProvinceName	给出个人所在的状态或省去。
streetaddress	为人的物理位置指定 street 名称和编号。
telephoneNumber	提供条目的电话号码。
teletexTerminalIdentifier	提供条目的 teletex 终端的 ID。
telexNumber	提供与条目关联的电话号。
title	显示个人的工作标题。
userPassword	存储条目可以绑定到目录的密码。
x121Address	为条目提供 X.121 地址。

9.98. ORGANIZATIONALROLE

organizationalRole 对象类用于定义机构中人员持有的角色的条目。

此对象类在 RFC 2256 中定义。

优越的类

top

OID

2.5.6.8

表 9.171. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
commonName	提供条目的通用名称。

表 9.172. 允许的属性

属性	定义
description	提供条目的文本描述。
destinationIndicator	提供与该条目关联的国家和城市；这一旦需要提供公共电话服务。
facsimileTelephoneNumber	包含条目的 fax 号。
internationalISDNNumber	包含条目的 ISDN 号。
localityName	提供条目的城市或地理位置。
organizationalUnitName	提供条目所属组织单元或部门。
physicalDeliveryOfficeName	提供可以进行物理分发的位置。
postalAddress	包含条目的电子邮件地址。
postalCode	提供条目的邮政代码，如美国的 zip 代码。
postOfficeBox	提供条目的 post office box 号码。
preferredDeliveryMethod	显示角色的首选联系方式或消息发送。
General_Atttribute_registeredAddress	当接收者必须验证交付时，提供适合接收快速文档的邮政地址。
roleOccupant	包含角色中个人的 DN （区分名称）。
seeAlso	包含指向另一个条目或站点的 URL，以及相关信息。
stateOrProvinceName	提供条目所在的状态或省去。
streetaddress	为角色物理位置指定 street 名称和数字。
telephoneNumber	提供条目的电话号码。

属性	定义
teletexTerminalIdentifier	提供条目的 teletex 终端的 ID。
telexNumber	提供与条目关联的电话号。
x121Address	为条目提供 X.121 地址。

9.99. ORGANIZATIONALUNIT

***organizationalUnit** 对象类定义代表 组织单元 的条目，通常理解在大型组织内成为相对静态分组。*

此对象类在 RFC 2256 中定义。

优越的类

top

OID

2.5.6.5

表 9.173. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
organizationalUnitName	提供条目所属组织单元或部门。

表 9.174. 允许的属性

属性	定义
businessCategory	给出了条目参与的商业类型。
description	提供条目的文本描述。
destinationIndicator	提供与该条目关联的国家和城市；这一旦需要提供公共电话服务。
facsimileTelephoneNumber	包含条目的 fax 号。

属性	定义
internationalISDNNumber	包含条目的 ISDN 号。
localityName	提供条目的城市或地理位置。
physicalDeliveryOfficeName	提供可以进行物理分发的位置。
postalAddress	包含条目的电子邮件地址。
postalCode	提供条目的邮政代码，如美国的 zip 代码。
postOfficeBox	提供条目的 post office box 号码。
preferredDeliveryMethod	给出要联系的首选方法。
General_Atttribute_registeredAddress	当接收者必须验证交付时，提供适合接收快速文档的邮政地址。
searchGuide	在将条目用作搜索的目录树中的基本对象时，指定推荐的搜索条件的信息。
seeAlso	包含指向另一个条目或站点的 URL，以及相关信息。
stateOrProvinceName	给出个人所在的状态或省去。
streetaddress	为角色物理位置指定 street 名称和数字。
telephoneNumber	提供条目的电话号码。
teletexTerminalIdentifier	提供条目的 teletex 终端的 ID。
telexNumber	提供与条目关联的电话号。
userPassword	存储条目可以绑定到目录的密码。
x121Address	为条目提供 X.121 地址。

9.100. 个人

***person** 对象类代表通用人员的条目。这是 **organizationalPerson** 对象类的基础对象类。*

此对象类在 RFC 2256 中定义。

优越的类

top

OID

2.5.6.6

表 9.175. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
commonName	提供条目的通用名称。
surname	提供个人的系列名称或姓氏。

表 9.176. 允许的属性

属性	定义
description	提供条目的文本描述。
seeAlso	包含指向另一个条目或站点的 URL，以及相关信息。
telephoneNumber	提供条目的电话号码。
userPassword	存储条目可以绑定到目录的密码。

9.101. PILOTOBJECT

pilotObject 是一个子类，允许将额外的属性分配给所有其他对象类的条目。

此对象类在 RFC 1274 中定义。

优越的类

top

OID

0.9.2342.19200300.100.4.3

表 9.177. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。

表 9.178. 允许的属性

属性	定义
audio	以二进制格式存储声音文件。
dITRedirect	包含用作条目的重定向的条目的 DN （区分名称）。
info	包含有关条目的信息。
jpegPhoto	存储 JPG 镜像。
lastModifiedBy	提供修改文档条目的最后一个用户的 DN （区分名称）。
lastModifiedTime	给出对象最近修改的时间。
Manager	提供条目管理器的 DN （区分名称）。
photo	以二进制格式存储文档的照片。
uniqueIdentifier	当可分辨名称被重复使用时，可以区分两个条目。

9.102. PILOTORGANIZATION

pilotOrganization 对象类是一个子类，用于向 organization 和 organizationalUnit 对象类条目添加属性。

此对象类在 RFC 1274 中定义。

优越的类

top

OID

0.9.2342.19200300.100.4.20

表 9.179. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
organizationName	提供条目所属的机构。
organizationalUnitName	提供条目所属组织单元或部门。

表 9.180. 允许的属性

属性	定义
buildingName	指定条目所在的构建的名称。
businessCategory	给出了条目参与的商业类型。
description	提供条目的文本描述。
destinationIndicator	提供与该条目关联的国家和城市；这一旦需要提供公共电话服务。
facsimileTelephoneNumber	包含条目的 fax 号。
internationalISDNNumber	包含条目的 ISDN 号。
localityName	提供条目的城市或地理位置。
physicalDeliveryOfficeName	提供可以进行物理分发的位置。
postalAddress	包含条目的电子邮件地址。
postalCode	提供条目的邮政代码，如美国的 zip 代码。
postOfficeBox	提供条目的 post office box 号码。
preferredDeliveryMethod	给出要联系的首选方法。
General_Atttribute_registeredAddress	当接收者必须验证交付时，提供适合接收快速文档的邮政地址。

属性	定义
searchGuide	在将条目用作搜索的目录树中的基本对象时，指定推荐的搜索条件的信息。
seeAlso	包含指向另一个条目或站点的 URL，以及相关信息。
stateOrProvinceName	给出个人所在的状态或省去。
streetaddress	为人的物理位置指定 street 名称和地址号。
telephoneNumber	提供条目的电话号码。
teletexTerminalIdentifier	提供条目的 teletex 终端的 ID。
telexNumber	提供与条目关联的电话号。
userPassword	存储条目可以绑定到目录的密码。
x121Address	为条目提供 X.121 地址。

9.103. PKICA

pkiCA 辅助对象类包含为证书颁发机构配置的必要或可用的证书。此对象类在 RFC 4523 中定义，它定义了用于管理 X.509 证书和相关证书服务的 LDAP 的对象类和属性。

优越的类

top

OID

2.5.6.22

表 9.181. 允许的属性

属性	定义
authorityRevocationList	包含已撤销 CA 证书的列表。
cACertificate	包含 CA 证书。
certificateRevocationList	包含已撤销的证书列表。

属性	定义
crossCertificatePair	包含一对证书，用于在 FBCA 风格的网桥 CA 配置中交叉认证对 CA 的证书。

9.104. PKIUSER

pkiUser 辅助对象类包含连接到公钥基础架构中证书颁发机构或元素的用户或客户端所需的证书。此对象类在 RFC 4523 中定义，它定义了用于管理 X.509 证书和相关证书服务的 LDAP 的对象类和属性。

优越的类

top

OID

2.5.6.21

表 9.182. 允许的属性

属性	定义
userCertificate	存储用户证书，通常采用二进制形式。

9.105. POSIXACCOUNT

posixAccount 对象类定义使用 POSIX 属性的网络帐户。此对象类在 RFC 2307 中定义，它定义了将 LDAP 用作网络信息服务的对象类和属性。

注意

此对象类在目录服务器中的 10rfc2307.ldif 中定义。要使用更新的 RFC 2307 模式，请删除 10rfc2307.ldif 文件，并将 10rfc2307bis.ldif 文件从 /usr/share/dirsrv/data 目录复制到 /etc/dirsrv/slapd-instance/schema 目录。

优越的类

top

OID

1.3.6.1.1.1.2.0

表 9.183. 必要属性

属性	定义
commonName	提供条目的通用名称。
gidNumber	包含组条目的唯一标识符，或者标识用户条目的组，类似于 Unix 中的组号。
homeDirectory	包含用户主目录的路径。
objectClass	提供分配给条目的对象类。
userID	提供定义的帐户用户 ID。
uidNumber	包含用户条目的唯一标识符，类似于 Unix 中的用户编号。

表 9.184. 允许的属性

属性	定义
description	提供条目的文本描述。
gecos	用于确定用户的 GECOS 字段；这是基于一个通用名称，其中嵌入了更多信息。
loginShell	包含用户在登录域时自动启动的脚本的路径。
userPassword	存储条目可以绑定到目录的密码。

9.106. POSIXGROUP

***posixGroup** 对象类定义使用 POSIX 属性的网络帐户组。此对象类在 RFC 2307 中定义，它定义了将 LDAP 用作网络信息服务的对象类和属性。*

优越的类

top

OID

1.3.6.1.1.1.2.2

表 9.185. 必要属性

属性	定义
gidNumber	包含用户在登录域时自动启动的脚本的路径。
objectClass	提供分配给条目的对象类。

表 9.186. 允许的属性

属性	定义
description	提供条目的文本描述。
memberUID	指定组成员的登录名称；这可能与成员的 DN 不同。
userPassword	包含组成员的登录名称。

9.107. REFERRAL

引用 对象类定义了一个对象，它支持 LDAPv3 智能引用。这个对象类在 LDAPv3 引用互联网 Draft 中定义。

优越的类

top

OID

2.16.840.1.113730.3.2.6

表 9.187. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。

表 9.188. 允许的属性

属性	定义
Ref	包含 LDAPv3 智能引用的信息。

9.108. RESIDENTIALPERSON

residentialPerson 对象类管理个人驻留的信息。

此对象类在 RFC 2256 中定义。

优越的类

top

OID

2.5.6.10

表 9.189. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
commonName	提供条目的通用名称。
localityName	提供条目的城市或地理位置。
surname	提供个人的系列名称或姓氏。

表 9.190. 允许的属性

属性	定义
businessCategory	给出了条目参与的商业类型。
description	提供条目的文本描述。
destinationIndicator	提供与该条目关联的国家和城市；这一旦需要提供公共电话服务。
facsimileTelephoneNumber	包含条目的 fax 号。

属性	定义
internationalISDNNumber	包含条目的 ISDN 号。
physicalDeliveryOfficeName	提供可以进行物理分发的位置。
postalAddress	包含条目的电子邮件地址。
postalCode	提供条目的邮政代码，如美国的 zip 代码。
postOfficeBox	提供条目的 post office box 号码。
preferredDeliveryMethod	显示人员的首选联系方式或消息发送。
General_Atttribute_registeredAddress	当接收者必须验证交付时，提供适合接收快速文档的邮政地址。
seeAlso	包含指向另一个条目或站点的 URL，以及相关信息。
stateOrProvinceName	给出个人所在的状态或省去。
streetaddress	为人的物理位置指定 street 名称和地址号。
telephoneNumber	提供条目的电话号码。
teletexTerminalIdentifier	提供条目的 teletex 终端的 ID。
telexNumber	提供与条目关联的电话号。
userPassword	存储条目可以绑定到目录的密码。
x121Address	为条目提供 X.121 地址。

9.109. RFC822LOCALPART

***RFC822LocalPart** 对象类定义代表 **RFC 8822** 邮件地址的本地部分的条目。目录将 **RFC822** 地址的这部分视为域。*

此对象类由 Internet Directory Pilot 定义。

优越的类

domain

OID

0.9.2342.19200300.100.4.14

表 9.191. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
dc	包含域名的一个组件。

表 9.192. 允许的属性

属性	定义
associatedName	指定与 DNS 域关联的组织目录树中的条目名称。
businessCategory	给出了条目参与的商业类型。
commonName	提供条目的通用名称。
description	提供条目的文本描述。
destinationIndicator	提供与该条目关联的国家和城市；这一旦需要提供公共电话服务。
facsimileTelephoneNumber	包含条目的 fax 号。
internationalISDNNumber	包含条目的 ISDN 号。
localityName	提供条目的城市或地理位置。
organizationName	提供帐户所属的机构。
physicalDeliveryOfficeName	提供可以进行物理分发的位置。
postalAddress	包含条目的电子邮件地址。
postalCode	提供条目的邮政代码，如美国的 zip 代码。
postOfficeBox	提供条目的 post office box 号码。
preferredDeliveryMethod	显示人员的首选联系方式或消息发送。

属性	定义
General_Atttribute_registeredAddress	当接收者必须验证交付时，提供适合接收快速文档的邮政地址。
searchGuide	在将条目用作搜索的目录树中的基本对象时，指定推荐的搜索条件的信息。
seeAlso	包含指向另一个条目或站点的 URL，以及相关信息。
surname	提供个人的系列名称或姓氏。
stateOrProvinceName	给出个人所在的状态或省去。
streetaddress	为人的物理位置指定 street 名称和地址号。
telephoneNumber	提供条目的电话号码。
teletexTerminalIdentifier	提供个人的 teletex 终端的标识符。
telexNumber	提供与条目关联的电话号。
userPassword	存储条目可以绑定到目录的密码。
x121Address	为条目提供 X.121 地址。

9.110. 房间

room 对象类将信息存储在有关房间的目录。

优越的类

top

OID

0.9.2342.19200300.100.4.7

表 9.193. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。

属性	定义
commonName	提供条目的通用名称。

表 9.194. 允许的属性

属性	定义
description	为房间提供文本描述。
roomNumber	包含房间号。
seeAlso	包含指向另一个条目或站点的 URL，以及相关信息。
telephoneNumber	提供条目的电话号码。

9.111. SHADOWACCOUNT

***shadowAccount** 对象类允许 **LDAP** 目录用作影子密码服务。影子密码服务将主机上的密码文件重新放置到具有严格限制访问权限的 **shadow** 文件。*

*此对象类在 **RFC 2307** 中定义，它定义了将 **LDAP** 用作网络信息服务的对象类和属性。*

注意

*此对象类在目录服务器中的 **10rfc2307.ldif** 中定义。要使用更新的 **RFC 2307** 模式，请删除 **10rfc2307.ldif** 文件，并将 **10rfc2307bis.ldif** 文件从 **/usr/share/dirsrv/data** 目录复制到 **/etc/dirsrv/slapd-instance/schema** 目录。*

优越的类

top

OID

1.3.6.1.1.1.2.1

表 9.195. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
userID	提供定义的帐户用户 ID。

表 9.196. 允许的属性

属性	定义
description	提供条目的文本描述。
shadowExpire	包含 shadow 帐户过期的日期。
shadowFlag	标识 shadow 映射中的哪些区域存储标志值。
shadowInactive	设置 shadow 帐户可以不活跃的时长。
shadowLastChange	包含对 shadow 帐户最后一次修改的时间和日期。
shadowMax	设置影子密码有效的最大天数。
shadowMin	设置在更改影子密码之间必须经过的最小天数。
shadowWarning	设置密码过期前的天数，以向用户发送警告。
userPassword	存储条目可以绑定到目录的密码。

9.112. SIMPLESECURITYOBJECT

*当条目的主体对象类不允许 **password** 属性时，**simpleSecurityObject** 对象类允许条目包含 **userPassword** 属性。保留供以后使用。*

此对象类在 RFC 1274 中定义。

优越的类

top

OID

0.9.2342.19200300.100.4.19

表 9.197. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
userPassword	存储条目可以绑定到目录的密码。

9.113. STRONGAUTHENTICATIONUSER

***strongAuthenticationUser** 对象类将用户的证书存储在 目录中。*

此对象类在 RFC 2256 中定义。

优越的类

top

OID

2.5.6.15

表 9.198. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。
userCertificate	存储用户证书，通常采用二进制形式。

第 10 章 操作属性和对象类

操作属性是用于执行目录操作的属性，并可用于目录中的每一条目，无论是否为条目的对象类定义它们。只有特别请求时，才会在 ldapsearch 操作中返回操作属性。要返回对象的所有操作属性，请指定 +。

操作属性由 Directory Server 在条目上创建和管理，如创建条目的时间以及创建者的名称。这些属性可以在任意条目上设置，无论条目上的其他属性或对象类如何。

10.1. ACCOUNTUNLOCKTIME

accountUnlockTime 属性包含帐户将被解锁的 GMT-format 的日期和时间。值 0 表示帐户必须由管理员解锁。

OID	2.16.840.1.113730.3.1.95
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	目录服务器

10.2. ACI

目录服务器使用此属性来评估从客户端接收 LDAP 请求时授予或拒绝哪些权限。

OID	2.16.840.1.113730.3.1.55
语法	IA5String
multi- 或 Single-Valued	多值
定义在	目录服务器

10.3. ALTSERVER

此属性的值是其他服务器的 URL，当这个服务器不可用时可以联系它们。如果服务器不知道可以使用的任何其他服务器，则缺少此属性。如果首选 LDAP 服务器稍后不可用，则可以缓存此信息。

OID	1.3.6.1.4.1.1466.101.120.6
语法	IA5String
multi- 或 Single-Valued	多值
定义在	RFC 2252

10.4. CREATETIMESTAMP

此属性包含条目初始创建的日期和时间。

OID	2.5.18.1
语法	GeneralizedTime
multi- 或 Single-Valued	单值
定义在	RFC 1274

10.5. CREATORSNAME

此属性包含创建条目的用户名称。

OID	2.5.18.3
语法	DN
multi- 或 Single-Valued	单值
定义在	RFC 1274

10.6. DITCONTENTRULES

此属性定义 subschema 中强制的 DIT 内容规则。每个值都定义一个 DIT 内容规则。每个值都由与它相关的 structural 对象类的对象标识符标记。

OID	2.5.21.2

语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2252

10.7. DITSTRUCTURERULES

此属性定义 subschema 中强制的 DIT 结构规则。每个值都定义一个 DIT 结构规则。

OID	2.5.21.1
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2252

10.8. ENTRYUSN

启用 USN 插件时，服务器会在每次执行写入操作（添加、修改、modrdn 或 delete）时自动为条目分配 更新序列号。USN 存储在条目上的 entryUSN 操作属性中；条目USN 会显示任何条目上最近更改的编号。

注意

entryUSN 属性仅与 LDAP 客户端执行的操作递增。它不计算内部操作。

默认情况下，条目USN 每个后端数据库实例都是唯一的，因此其他数据库中的条目可能具有相同的 USN。nsslapd-entryusn-global 参数将 USNs 的分配从 local 改为 global，即从计算在单个数据库上进行计数，以计算拓扑中所有数据库。参数默认为关闭。

对应的条目 lastusn 保存在 root DSE 条目中，其中显示了最近分配的 USN。在本地 模式中，lastusn 显示每个后端数据库最近分配的 USN。在 全局 模式中，lastusn 显示整个拓扑最近分配的 USN。

OID	2.16.840.1.113730.3.1.606
语法	整数

multi- 或 Single-Valued	单值
定义在	目录服务器

10.9. GLUE

glue 对象类定义一个处于特殊状态的条目：由于复制冲突，重新执行。

此对象类由 Directory Server 定义。

优越的类

top

OID

2.16.840.1.113730.3.2.30

表 10.1. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。

10.10. HASSUBORDINATES

此属性指示条目是否具有下级条目。

OID	1.3.6.1.4.1.1466.115.121.1.7
语法	布尔值
multi- 或 Single-Valued	单值
定义在	numSubordinates Internet Draft

10.11. INTERNALCREATORSNAME

对于插件或服务器创建的条目，而不是目录服务器用户，此属性记录内部用户（按插件 DN）创建条目。

internalCreatorsname 属性始终将插件显示为身份。此插件可以是额外的插件，如 MemberOf 插件。如果更改由核心目录服务器进行，则插件是数据库插件 cn=ldbm database,cn=plugins,cn=config。

OID	2.16.840.1.113730.3.1.2114
语法	DN
multi- 或 Single-Valued	单值
定义在	目录服务器

10.12. INTERNALMODIFIERSNAME

如果一个条目由插件或服务器编辑，而不是目录服务器用户，此属性记录内部用户（通过插件 DN）修改该条目。

internalModifiersname 属性始终将插件显示为身份。此插件可以是额外的插件，如 MemberOf 插件。如果更改由核心目录服务器进行，则插件是数据库插件 cn=ldbm database,cn=plugins,cn=config。

OID	2.16.840.1.113730.3.1.2113
语法	DN
multi- 或 Single-Valued	单值
定义在	目录服务器

10.13. LASTLOGINTIME

lastLoginTime 属性包含给定帐户对目录进行身份验证的最后一次时间的时间戳，格式为 YYYMMDDHHMMSSZ。例如：

```
lastLoginTime: 20200527001051Z
```

这用于根据帐户不活跃评估帐户锁定策略。

OID	2.16.840.1.113719.1.1.4.1.35
语法	GeneralizedTime
multi- 或 Single-Valued	单值
定义在	目录服务器

10.14. LASTMODIFIEDBY

lastModifiedBy 属性包含最后一次编辑条目的用户的可分辨名称(DN)。例如：

> ***lastModifiedBy: cn=Barbara Jensen,ou=Engineering,dc=example,dc=com***

OID	0.9.2342.19200300.100.1.24
语法	DN
multi- 或 Single-Valued	多值
定义在	RFC 1274

10.15. LASTMODIFIEDTIME

lastModifiedTime 属性包含以 UTC 格式的时间，条目上次修改。例如：

> ***lastModifiedTime: Thursday, 22-Sep-93 14:15:00 GMT***

OID	0.9.2342.19200300.100.1.23
语法	DirectyString
multi- 或 Single-Valued	多值
定义在	RFC 1274

10.16. LDAPSUBENTRY

这些条目存放操作数据。此对象类在 LDAP Subentry Internet Draft 中定义。

优越的类

top

OID

2.16.840.1.113719.2.142.6.1.1

表 10.2. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。

表 10.3. 允许的属性

属性	定义
commonName	指定条目的通用名称。

10.17. LDAPSYNTAXES

此属性标识实施的语法，每个值对应一个语法。

OID	1.3.6.1.4.1.1466.101.120.16
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2252

10.18. MATCHINGRULES

此属性定义子schema 中使用的匹配规则。每个值都定义一个匹配的规则。

OID	2.5.21.4
语法	DirectoryString

multi- 或 Single-Valued	多值
定义在	RFC 2252

10.19. MATCHINGRULEUSE

此属性指示在 subschema 中匹配规则应用到的属性类型。

OID	2.5.21.8
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2252

10.20. MODIFIERSNAME

此属性包含最后一次修改条目的用户名称。

OID	2.5.18.4
语法	DN
multi- 或 Single-Valued	单值
定义在	RFC 1274

10.21. MODIFYTIMESTAMP

此属性包含条目最近修改的日期和时间。

OID	2.5.18.2
语法	GeneralizedTime
multi- 或 Single-Valued	单值
定义在	RFC 1274

10.22. NAMEFORMS

此属性定义子schema 中使用的名称表单。每个值都定义一个名称表单。

OID	2.5.21.7
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	RFC 2252

10.23. NSACCOUNTLOCK

此属性显示帐户是活跃的还是不活跃。

OID	2.16.840.1.113730.3.1.610
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	目录服务器

10.24. NSAIMSTATUSGRAPHIC

此属性包含一个指向图形的路径， 它演示了 AIM 用户状态。

OID	2.16.840.1.113730.3.1.2018
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	目录服务器

10.25. NSAIMSTATUSTEXT

此属性包含指示当前 AIM 用户状态的文本。

OID	2.16.840.1.113730.3.1.2017
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	目录服务器

10.26. NSBACKENDSUFFIX

它包含后端使用的后缀。

OID	2.16.840.1.113730.3.1.803
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	目录服务器

10.27. NSCPENTRYDN

此属性包含 tombstone 条目的(former)条目 DN。

OID	2.16.840.1.113730.3.1.545
语法	DN
multi- 或 Single-Valued	单值
定义在	目录服务器

10.28. NSDS5REPLCONFLICT

此属性包含在具有更改冲突的条目中，这些冲突无法通过同步或复制过程自动解决。nsDS5ReplConflict 的值包含有关冲突哪些条目的信息，通常是通过使用当前条目和 tombstone 条目的 nsUniqueID 引用它们。

OID	2.16.840.1.113730.3.1.973
语法	DirectoryString
multi- 或 Single-Valued	多值
定义在	目录服务器

10.29. NSICQSTATUSGRAPHIC

此属性包含一个指向图形的路径，它演示了 ICQ 用户状态。

OID	2.16.840.1.113730.3.1.2022
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	目录服务器

10.30. NSICQSTATUSTEXT

此属性包含当前 ICQ 用户状态的文本。

OID	2.16.840.1.113730.3.1.2021
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	目录服务器

10.31. NSIDLETIMEOUT

此属性标识基于用户的连接闲置超时时间，以秒为单位。

OID	2.16.840.1.113730.3.1.573
语法	整数

multi- 或 Single-Valued	单值
定义在	目录服务器

10.32. NSIDLISTSCANLIMIT

此属性指定搜索在搜索操作过程中搜索的条目 ID 数量。保留默认值以提高搜索性能。

OID	2.16.840.1.113730.3.1.2106
语法	整数
multi- 或 Single-Valued	单值
定义在	目录服务器

10.33. NSLOOKTHROUGHLIMIT

此属性设置允许服务器在搜索操作中查找该用户的最大条目数。此属性在服务器本身中配置，并在用户启动搜索时应用到用户。

OID	2.16.840.1.113730.3.1.570
语法	整数
multi- 或 Single-Valued	单值
定义在	目录服务器

10.34. NSPAGEDIDLISTSCANLIMIT

此属性指定搜索的条目 ID 数量，特别是使用简单页面的结果控制的搜索操作。此属性的工作方式与 nsIDListScanLimit 属性相同，但它只适用于使用简单的页面结果控制进行搜索。

如果此属性不存在或设为零，则使用 nsIDListScanLimit 来分页搜索和非页式搜索。

OID	2.16.840.1.113730.3.1.2109

语法	整数
multi- 或 Single-Valued	单值
定义在	目录服务器

10.35. NSPAGEDLOOKTHROUGHLIMIT

此属性指定目录服务器在检查使用简单页面结果控制的候选条目时检查的最大条目数。此属性的工作方式与 nsLookThroughLimit 属性相同，但它只适用于使用简单的页面结果控制进行搜索。

如果此属性不存在或设为零，则使用 nsLookThroughLimit 来分页搜索和非页式搜索。

OID	2.16.840.1.113730.3.1.2108
语法	整数
multi- 或 Single-Valued	单值
定义在	目录服务器

10.36. NSPAGEDSIZELIMIT

此属性设置从搜索操作返回的最大条目数，特别是使用简单页面的结果控制。这会覆盖 paged 搜索的 nsSizeLimit 属性。

如果将此值设置为零，则使用 nsSizeLimit 属性进行分页搜索，以及使用全局配置设置。

OID	2.16.840.1.113730.3.1.2107
语法	整数
multi- 或 Single-Valued	单值
定义在	目录服务器

10.37. NSPARENTUNIQUEID

对于存储在复制中的 tombstone （删除）条目，nsParentUniqueId 属性包含原始条目的父 DN 或条目 ID。

OID	2.16.840.1.113730.3.1.544
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	目录服务器

10.38. NSROLE

此属性是没有与条目本身存储的 computed 属性。它标识条目所属的角色。

OID	2.16.840.1.113730.3.1.574
语法	DN
multi- 或 Single-Valued	多值
定义在	目录服务器

10.39. NSROLEDN

此属性包含应用到条目的所有角色的可分辨名称。通过将角色的 DN 添加到条目的 nsRoleDN 属性来授予受管角色的成员。例如：

```
dn: cn=staff,ou=employees,dc=example,dc=com
objectclass: LDAPsubentry
objectclass: nsRoleDefinition
objectclass: nsSimpleRoleDefinition
objectclass: nsManagedRoleDefinition

dn: cn=userA,ou=users,ou=employees,dc=example,dc=com
objectclass: top
objectclass: person
sn: uA
userpassword: secret
nsroledn: cn=staff,ou=employees,dc=example,dc=com
```

嵌套角色指定任何类型的一个或多个角色的包含。在这种情况下，nsRole DN 定义包含角色的 DN。例如：

```
dn: cn=everybody,ou=employees,dc=example,dc=com
objectclass: LDAPsubentry
objectclass: nsRoleDefinition
objectclass: nsComplexRoleDefinition
objectclass: nsNestedRoleDefinition
nsroledn: cn=manager,ou=employees,dc=example,dc=com
nsroledn: cn=staff,ou=employees,dc=example,dc=com
```

OID	2.16.840.1.113730.3.1.575
语法	DN
multi- 或 Single-Valued	多值
定义在	目录服务器

10.40. NSROLEFILTER

此属性设置过滤器标识属于该角色的条目。

OID	2.16.840.1.113730.3.1.576
语法	IA5String
multi- 或 Single-Valued	单值
定义在	RFC 2252

10.41. NSSCHEMACSN

此属性是 subschema DSE 属性类型之一。

OID	2.5.21.82.16.840.1.113730.3.1.804
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	目录服务器

10.42. NSSIZELIMIT

此属性以字节为单位显示数据库或数据库链接的默认大小限制。

OID	2.16.840.1.113730.3.1.571
语法	整数
multi- 或 Single-Valued	单值
定义在	目录服务器

10.43. NSTIMELIMIT

此属性显示数据库或数据库链接的默认搜索时间限制。

OID	2.16.840.1.113730.3.1.572
语法	整数
multi- 或 Single-Valued	单值
定义在	目录服务器

10.44. NSTOMBSTONE （对象类）

tombstone 条目是已从 Directory Server 中删除的条目。对于复制和恢复操作，这些删除的条目会被保存，以便在需要时可以重新处理和替换它们。每个 tombstone 条目都自动具有 nsTombstone 对象类。

此对象类在 Directory Server 中定义。

优越的类

top

OID

2.16.840.1.113730.3.2.113

表 10.4. 必要属性

属性	定义
objectClass	提供分配给条目的对象类。

表 10.5. 允许的属性

属性	定义
nsParentUniqueId	标识原始条目的父条目的唯一 ID。
nscpEntryDN	在 tombstone 条目中标识 orignal 条目 DN。

10.45. NSUNIQUEID

此属性标识或分配唯一 ID 到服务器条目。

OID	2.16.840.1.113730.3.1.542
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	目录服务器

10.46. NSYIMSTATUSGRAPHIC

此属性包含一个指向图形的路径，它演示了 Yahoo IM 用户状态。

OID	2.16.840.1.113730.3.1.2020
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	目录服务器

10.47. NSYIMSTATUSTEXT

此属性包含当前 Yahoo IM 用户状态的文本。

OID	2.16.840.1.113730.3.1.2019
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	目录服务器

10.48. NUMSUBORDINATES

此属性指示现在很多直接从属条目具有。例如， leaf entry 中的 numSubordinates=0。

OID	1.3.1.1.4.1.453.16.2.103
语法	整数
multi- 或 Single-Valued	单值
定义在	numSubordinates Internet Draft

10.49. PASSWORDGRACEUSERTIME

此属性统计用户用过期密码进行的尝试次数。

OID	2.16.840.1.113730.3.1.998
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	目录服务器

10.50. PASSWORDOBJECT （对象类）

此对象类用于在 目录中存储用户的密码信息的条目。

此对象类在 Directory Server 中定义。

优越的类

top

OID

2.16.840.1.113730.3.2.12

表 10.6. 必要属性

objectClass	定义条目的对象类。

表 10.7. 允许的属性

accountUnlockTime	指的是在帐户锁定后必须经过的时间，用户才能再次绑定到该目录。
passwordAllowChangeTime	指定在允许用户更改密码前必须经过的时长。
password_ExpirationTime	指定在用户的密码过期前通过的时间长度。
password_ExpWarned	表示密码到期警告已发送给用户。
passwordGrace_UserTime	指定在密码过期后允许用户的登录尝试次数。
cnconfig-passwordHistory_Password_History	包含用户之前密码的历史记录。
password_RetryCount	计算输入正确密码时连续失败的尝试数量。
pwdpolicy_subentry	指向新密码策略的条目 DN。
retryCountResetTime	指定在重置 **passwordRetryCount** 属性前传递的时间长度。

10.51. PASSWORDRETRYCOUNT

此属性计算输入正确密码时连续失败的尝试数量。

OID	2.16.840.1.113730.3.1.93
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	目录服务器

10.52. PWDPOLICYSUBENTRY

这个属性值指向新密码策略的条目 DN。

OID	2.16.840.1.113730.3.1.997
语法	DirectoryString
multi- 或 Single-Valued	单值
定义在	目录服务器

10.53. PWDUPDATETIME

此属性值存储帐户最近更改密码的时间。

OID	2.16.840.1.113730.3.1.2133
语法	GeneralizedTime
multi- 或 Single-Valued	单值
定义在	目录服务器

10.54. SUBSCHEMA （对象类）

这标识了辅助对象类子条目，它管理子schema 管理区域的子schema。它包含代表代表 subschema 的策略参数的操作属性。

此对象类在 RFC 2252 中定义。

优越的类

top

OID

2.5.20.1

表 10.8. 必要属性

objectClass	定义条目的对象类。

表 10.9. 允许的属性

attributeTypes	subschema 中使用的属性类型。
dITContentRules	定义 subschema 中强制使用的 DIT 内容规则。
dITStructureRules	定义 subschema 中强制使用的 DIT 结构规则。
matchingRuleUse	表示在 subschema 中匹配规则应用到的属性类型。
matchingRules	定义子方案中使用的匹配规则。
nameForms	定义 subschema 中使用的名称表单。
objectClasses	定义子schema 中使用的对象类。

10.55. SUBSCHEMASUBENTRY

此属性包含包含 schema 信息的条目的 DN。例如：

```
subschemaSubentry: cn=schema
```

OID	2.5.18.10
语法	DN
multi- 或 Single-Valued	单值
定义在	RFC 2252

第 11 章 日志文件参考

目录服务器将事件记录到日志文件，对于解决现有问题和预测潜在问题至关重要，这可能会导致性能失败或不佳。

使用日志文件，您可以实现以下目标：

- 对问题进行故障排除。
- 监控服务器活动。
- 分析目录活动。

要有效地监控目录，您必须了解日志文件的结构和内容。

您没有在章节中找到日志消息的详细列表。提供的信息是解决常见问题的良好起点，并了解访问、错误、审计、审计失败和安全日志中记录。

目录服务器实例将日志存储在 /var/log/dirsrv/slapd-instance_name 目录中。

11.1. 访问日志参考

目录服务器访问日志包含有关与目录的客户端连接的详细信息。连接是来自同一客户端的请求序列，结构如下：

- 提供连接索引和客户端的 IP 地址的连接记录
- 绑定记录
- 绑定结果记录

- 连接、关闭和带外记录时一系列操作请求和操作结果对记录或单个记录
- 取消绑定记录
- 关闭的记录

访问日志记录示例：

```
[time_stamp] conn=1 op=73 SRCH base="dc=example,dc=com" scope=2 filter="(&
(objectClass=top)(objectClass=ldapsubentry)(objectClass=passwordpolicy))"
attrs="distinguishedName"
[time_stamp] conn=1 op=73 RESULT err=0 tag=101 nentries=24 wtime=0.000078414
optime=0.001614101 etime=0.001690742
```

几乎所有记录都出现在对中：一个服务请求记录，在示例中是 SRCH，后跟一个 RESULT 记录。连接、关闭和带包记录单独出现。

访问日志有几个级别的日志记录，您可以使用 nsslapd-accesslog-level 属性进行配置。

11.1.1. 访问日志记录级别

不同的访问日志记录级别，记录目录服务器执行的不同类型的操作。

访问日志有以下日志级别：

- 无访问日志记录(0)。
- 内部访问操作的日志记录(4)。
- 记录连接、操作和结果(256)。默认级别。
- 记录以访问条目和引用(512)。

使用 nsslapd-accesslog-level 属性配置访问日志级别。属性值是 additive：如果您设置了日志级别值 260，它包含级别 256 和 4。

其他资源

- 配置日志级别
- lapd-accesslog-level 属性的描述

11.1.2. 默认访问日志内容

默认情况下，Directory 服务器具有 256 日志记录级别，记录对条目的访问权限，并且包含进一步介绍的信息。

连接号(conn)

目录服务器列出了示例中带有增量连接号 conn=13 的每个外部 LDAP 请求。连接编号在服务器启动后立即从 conn=0 开始。

> [time_stamp] conn=13 fd=608 slot=608 connection from 172.17.0.2 to 172.17.0.2

默认情况下，目录服务器不会记录内部 LDAP 请求。要启用内部访问操作的日志记录，请使用 nsslapd-accesslog-level 配置属性。

文件描述符(fd)

每个从外部 LDAP 客户端连接到目录服务器都需要来自操作系统的文件描述符或套接字描述符，本例中为 fd=608。fd=608 值表示外部 LDAP 客户端使用文件描述符编号为可用文件描述符总数的 608。

> [time_stamp] conn=11 fd=608 slot=608 connection from 172.17.0.2 to 172.17.0.2

插槽号(slot)

示例中的插槽号 slot=608 是访问日志的传统部分，其含义与文件描述符相同。忽略访问日志的这一部分。

> [time_stamp] conn=11 fd=608 slot=608 connection from 172.17.0.2 to 172.17.0.2.

操作号(opt)

要处理 LDAP 请求，目录服务器执行一系列操作。对于连接，所有操作请求和操作结果对都有一个增量操作号，以 op=0 开头来识别不同的操作。

```
[time_stamp] conn=14 op=0 BIND dn="cn=Directory Manager" method=128 version=3
[time_stamp] conn=14 op=0 RESULT err=0 tag=97 nentries=0 wtime=0.000076581
optime=0.000082736 etime=0.000158680
[time_stamp] conn=14 op=1 SRCH base="dc=example,dc=com" scope=2 filter="
(uid=bjensen)"
[time_stamp] conn=14 op=2 ABANDON targetop=2 msgid=3 nentries=0 etime=0.0000113702
[time_stamp] conn=14 op=3 UNBIND
[time_stamp] conn=14 op=3 fd=634 closed - U1
```

在示例中：

- *bind 操作请求的 op=0 和结果*
- *用于 LDAP 搜索请求的 op=1 和结果*
- *op=2 用于 abandon 操作*
- *op=3 用于 LDAP 客户端发送的未绑定操作和结果*

方法类型(method)

示例中的方法号 method=128 表示客户端使用的 LDAPv3 绑定方法。

```
[time_stamp] conn=11 op=0 BIND dn="cn=Directory Manager" method=128 version=3
```

方法类型可以有三个可能的值之一：

- *0 用于身份验证*
- *128 用于通过用户密码进行简单绑定*

- *使用外部身份验证机制的 SASL 绑定*

版本号（版本）

版本号表示 LDAP 客户端用于与 LDAP 服务器通信的 LDAP 版本号。LDAP 版本号可以是 LDAPv2 或 LDAPv3。在示例中，它使用 version=3。

> *[time_stamp] conn=11 op=0 BIND dn="cn=Directory Manager" method=128 version=3*

错误编号(err)

错误号提供返回执行 LDAP 操作的 LDAP 结果代码。LDAP 错误号 0 表示操作成功。该示例具有 op=0。

> *[time_stamp] conn=2 op=0 RESULT err=0 tag=97 nentries=0 wtime=0.000076581 optime=0.000082736 etime=0.000158680*

标签号（标签）

标签号表示操作返回的结果的类型。目录服务器使用 LDAP 协议中的 BER 标签。示例具有 tag=97。

> *[time_stamp] conn=11 op=0 RESULT err=0 tag=97 nentries=0 wtime=0.000076581 optime=0.000082736 etime=0.000158680*

下表提供了常用的标签：

标签	描述
tag=97	客户端绑定操作的结果。
tag=100	Directory 服务器搜索的实际条目。这不是结果标签，访问日志不包含这样的标签。
tag=101	搜索操作的结果。
tag=103	修改操作的结果。
tag=105	添加操作的结果。
tag=107	删除操作的结果。
tag=109	来自 moddn （重命名）操作的结果。

标签	描述
tag=111	比较操作的结果。
tag=115	当操作搜索的条目包含所需条目的引用时，搜索引用。这不是结果标签，访问日志不包含这样的标签。
tag=120	扩展操作的结果。
tag=121	中间操作的结果。

条目数(nentries)

nentries 记录显示搜索操作与 LDAP 客户端请求匹配的条目数。

> ***[time_stamp] conn=11 op=0 RESULT err=0 tag=97 nentries=0 wtime=0.000076581 optime=0.000082736 etime=0.000158680***

在示例中，nentries=0 找不到任何匹配的条目。

已经过的时间(etime)

etime 记录显示目录服务器执行 LDAP 操作所花费的时间或时间（以秒为单位）。

> ***[time_stamp] conn=11 op=1 RESULT err=0 tag=101 nentries=1 wtime=0.000076581 optime=0.000082736 etime=0.000158680 notes=U***

在示例中，目录服务器花费 0.000158680 秒来执行该操作。

etime 值 0 表示操作实际上需要 0 纳秒才能执行。

LDAP 请求类型

LDAP 请求类型指示发出的 LDAP 请求 LDAP 客户端的类型。可能的值有：

- ***SRCH 用于搜索操作***

- MOD 用于修改操作
- DEL 用于删除操作
- add 操作的 ADD
- MODDN for a moddn (renaming)操作
- EXT 用于扩展操作
- 用于带外操作的 ABANDON
- 如果 LDAP 请求结果对条目排序，则 SORT serialno

> [time_stamp] conn=114 op=68 SORT serialno (1)

在示例中，以括号括起的数字指定 LDAP 请求排序了一个候选条目。

LDAP 响应类型

目录服务器可以发出三个 LDAP 响应类型：

- RESULT 表示客户端 LDAP 请求的结果。
- ENTRY 表示条目目录服务器返回以响应搜索操作。
- REFERRAL 表示目录服务器将 LDAP 请求发送到另一台服务器。

RESULT 消息包含以下与性能相关的记录：

wtime

在 worker 线程获取操作前，操作在工作队列中等待的时间

optime

执行任务的实际操作所需的时间

etime

目录服务器接收请求和服务器何时将结果发回到客户端之间的时间。

注意

wtime 和 optime *值提供有关服务器如何处理负载和进程操作的有用信息。由于目录服务器需要一些时间来收集这些统计数据，因此* **wtime 和 optime** *值的总和比* **etime** *值稍长。*

搜索指标（注）

目录服务器提供有关在日志条目的备注消息中搜索的附加信息。例如：

```
[time_stamp] conn=11 op=1 RESULT err=0 tag=101 nentries=1 wtime=0.000076581
optime=0.000082736 etime=0.000158680 notes=U
```

目录服务器支持以下搜索指示符：

搜索指示符	描述
notes=P	分页的搜索指示器。有限资源的 LDAP 客户端可以控制 LDAP 服务器返回搜索操作结果的速率。当执行的搜索使用 LDAP 控制扩展进行简单搜索结果分页时，Directory 服务器会记录 **notes=P** paged 搜索指示符。这个指示符是信息，不需要进一步的操作。有关页搜索指标的详情，请参阅 RFC 2696 规格。
notes=A	未索引的搜索指示符。当过滤器中的所有候选属性都未索引且需要完整表扫描时，目录服务器会记录 **notes=A**。这可以超过 **nsslapd-lookthroughlimit** 属性中设置的值。

搜索指示符	描述
notes=U	未索引的搜索指示符。在以下情况下，目录服务器会记录 **notes=U** ： • 至少一个搜索术语是 unindexed。 • 搜索操作超过 **nsslapd-idlistscanlimit** 属性中设置的限制。
notes=F	未知属性指示符。当搜索过滤器包含未知属性时，目录服务器会记录 **notes=F**。
notes=M	MFA 插件绑定指示符。当您使用预绑定身份验证插件（如 MFA 插件）为用户帐户配置双因素身份验证时，目录服务器会记录 **notes=M**。

*请注意记录可以包括值的组合： **notes=P,A** 和 **notes=U,P**。*

如果没有索引属性， Directory 服务器必须直接在数据库中搜索它们。这个过程比搜索索引文件更多的资源密集型。

在以下情况下会出现未索引搜索：

- *即使使用 index 文件，搜索操作也会超过 **nsslapd-idlistscanlimit** 属性中设置的搜索条目数量。有关 **nsslapd-idlistscanlimit** 属性的详情，请参阅 nsslapd-idlistscanlimit 描述*
- *不存在索引文件。*
- *搜索需要的方式没有配置索引文件。*

要优化将来的搜索，请在索引中添加经常搜索的未索引属性。

注意

*不索引的搜索指示器通常附带一个大的 **etime** 值，因为未索引的搜索通常更耗时。*

MFA 插件绑定

当您使用 pre-bind 身份验证插件（如 MFA 插件）为用户帐户配置双因素身份验证时，访问日志记录将 notes=M 备注消息记录到文件中：

```
[time_stamp] conn=1 op=0 BIND dn="uid=jdoe,ou=people,dc=example,dc=com" method=128
version=3
[time_stamp] conn=1 op=0 RESULT err=0 tag=97 nentries=0 wtime=0.000111632
optime=0.006612223 etime=0.006722325 notes=M details="Multi-factor Authentication"
dn="uid=jdoe,ou=people,dc=example,dc=com"
```

注意

要使访问日志记录 notes=M 记录消息，则 pre-bind 身份验证插件必须使用 SLAPI API 设置标记（如果绑定是此插件的一部分）。

VLV 相关条目(VLV)

当搜索涉及虚拟列表视图(VLV)时，Directory 服务器会将适当的条目记录到访问日志文件。与其他条目类似，VLV 特定的记录将分别显示请求和响应信息：

```
[time_stamp] conn=67 op=8530 VLV 0:5:0210 10:5397 (0)
```

在示例中，请求信息为 0:5:0210，其格式为 beforeCount:afterCount:index:contentCount。响应信息为 10:5397 (0)，格式为 targetPosition:contentCount (resultCode)。

如果客户端使用位置值 VLV 请求，则请求信息格式是 beforeCount: afterCount: value。

搜索范围（范围）

scope 条目定义了执行的搜索操作的范围，并可具有以下值之一：

- *0 用于基础搜索*
- *1 用于单级搜索*
- *2 用于子树搜索*

扩展操作 OID (oid)

oid 记录提供已执行扩展操作的对象标识符(OID)。以下是使用扩展操作 OID 访问日志记录示例：

```
[time_stamp] conn=13 op=1 EXT oid="2.16.840.1.113730.3.5.3"
...
[time_stamp] conn=15 op=3 EXT oid="2.16.840.1.113730.3.5.5"
```

目录服务器支持以下 LDAPv3 扩展操作列表及其 OID：

扩展操作名称	描述	OID
目录服务器启动复制请求	复制启动器请求复制会话。	2.16.840.1.113730.3.5.3
目录服务器复制响应	复制响应器以响应 Start Replication Request 扩展操作或 End Replication Request 扩展操作。	2.16.840.1.113730.3.5.4
目录服务器结束复制请求	复制启动器终止复制会话。	2.16.840.1.113730.3.5.5
目录服务器复制条目请求	传输包含状态信息(**csn** 和 **UniqueIdentifier**)的条目，用于执行副本初始化。	2.16.840.1.113730.3.5.6
目录服务器 Bulk Import Start	客户端使用 Bulk Import Start 操作与导入的后缀一起请求批量导入，Directory 服务器则表示批量导入可能会开始。	2.16.840.1.113730.3.5.7
目录服务器 Bulk Import Finished	客户端使用 Bulk Import Finished 操作结束批量导入，目录服务器确认批量导入结束。	2.16.840.1.113730.3.5.8

更改序列号(csn)

csn 消息（如 csn=3b4c8cfb000000030000 ）表示 Directory 服务器收到由其"csn"标识的更新并处理它。

Abandon message (ABANDON)

abandon 消息表示客户端或 Directory 服务器终止一个操作。

以下是包含 abandon 消息的日志记录示例：

```
[time_stamp] conn=12 op=1 SRCH base="dc=example,dc=com" scope=2 filter="
(uid=bjensen)"
[time_stamp] conn=12 op=2 ABANDON targetop=2 msgid=3 nentries=0 etime=0.0000113980
```

nentries=0 值指示在操作终止前发送的条目服务器数量，etime=0.0000113980 值指示已经过的时间（以秒为单位），targetop=2 对应于 Directory 服务器前面启动的操作号(opt=2)。

如果目录服务器找不到 abandon 的操作，则日志记录包含 targetop=NOTFOUND 信息：

```
[time_stamp] conn=12 op=2 ABANDON targetop=NOTFOUND msgid=2
```

示例消息表示目录服务器已在之前完成操作，或者是一个未知的操作。

消息 ID (msgid)

LDAP SDK 客户端生成消息 ID，如 msgid=2，这也是 LDAP 操作标识符。msgid 值可能与 opt 值不同，但它标识相同的操作。目录服务器记录带有 ABANDON 操作的 msgid，并告知用户哪些客户端操作被取消：

```
[time_stamp] conn=12 op=2 ABANDON targetop=NOTFOUND msgid=2
```

注意

对于连接，目录服务器操作号选择从 0 开始计算。在大多数 LDAP SDK/客户端实现中，消息 ID 号 msgid 开始计算为 1。这解释了 msgid 经常等于 Directory 服务器选择加上 1 的原因。

SASL 多阶段绑定日志记录

目录服务器记录绑定进程的每个阶段。SASL 连接的错误代码实际上是返回代码：

```
[time_stamp] conn=16 op=0 BIND dn="" method=sasl version=3 mech=DIGEST-MD5
[time_stamp] conn=16 op=0 RESULT err=14 tag=97 nentries=0 wtime=0.000076581
optime=0.000082736 etime=0.000158680, SASL bind in progress
```

示例记录表示 SASL 绑定当前正在进行中（在进行中SASL 绑定），并且返回码为 err=14。这意味着连接仍然处于打开状态。目录服务器记录 SASL 将信息与 LDAP 版本号(version=3)绑定，并使用 SASL

机制(mech=DIGEST-MD5)。

注意

因为 SASL 身份验证需要多个步骤，所以目录服务器在 Directory 服务器完成绑定进程时，将经过身份验证的 DN （用于访问控制决策的 DN）记录在 bind RESULT 行中。这显示了映射到 SASL 绑定请求的条目：

```
[time_stamp] conn=14 op=1 RESULT err=0 tag=97 nentries=0
wtime=0.000076581 optime=0.000082736 etime=0.000158680
dn="uid=jdoe,dc=example,dc=com"
```

11.1.3. 非默认访问日志内容

当您设置非默认日志级别或应用特定的日志配置时，目录服务器开始将其他信息记录到访问日志文件中。

内部操作记录

当您为内部操作启用日志记录时，Directory 服务器开始记录由 Directory 服务器或客户端启动的内部操作。

服务器发起的内部操作

如果客户端删除了条目，服务器会运行多个内部操作，如查找条目并更新用户所属的组。

以下示例显示了服务器发起的内部操作日志格式：

```
[time_stamp] conn=Internal(0) op=0(0)(0) MOD dn="cn=uniqueid generator,cn=config"
[time_stamp] conn=Internal(0) op=0(0)(0) RESULT err=0 tag=48 nentries=0
wtime=0.0003979676 optime=0.0003989250 etime=0.0007968796
```

示例记录具有 conn=Internal，后跟 (0) 和 op=0 (nesting_level)。操作 ID 和内部操作 ID 始终为 0。对于非嵌套日志记录，嵌套级别为 0。

客户端发起的内部操作

客户端发起的内部操作日志除执行搜索的详细信息外还具有搜索基础、范围、过滤器和请求的搜索属性。以下示例显示了日志记录的格式：

```
[time_stamp] conn=5 (Internal) op=15(1)(0) SRCH base="cn=config,cn=userroot,cn=ldbm
database,cn=plugins,cn=config" scope=1 filter="objectclass=vlvsearch" attrs=ALL
[time_stamp] conn=5 (Internal) op=15(1)(0) RESULT err=0 tag=48 nentries=0
wtime=0.0000143989 optime=0.0000151450 etime=0.0000295419
[time_stamp] conn=5 (Internal) op=15(2)(0) SRCH base="cn=config,cn=example,cn=ldbm
database,cn=plugins,cn=config" scope=1 filter="objectclass=vlvsearch" attrs=ALL
[time_stamp] conn=5 (Internal) op=15(2)(0) RESULT err=0
```

示例记录具有 conn 记录，它被设置为客户端连接 ID，后跟字符串 (Internal)。op 记录包含操作 ID，后跟 (internal_operation_ID) (nesting_level)。内部操作 ID 可能有所不同。对于非嵌套日志条目，嵌套级别为 0。

启用插件日志记录的内部操作

如果将 nsslapd-plugin-logging 参数设置为 on，且启用了内部操作日志记录(4)，Directory 服务器还会记录插件的内部操作。

例如，如果您删除了 uid=user,dc=example,dc=com 条目，而 Referential Integrity 插件会自动从 example 组中删除此条目，服务器会记录以下内容：

```
[time_stamp] conn=2 op=37 DEL dn="uid=user,dc=example,dc=com"
[time_stamp] conn=2 (Internal) op=37(1) SRCH base="uid=user,dc=example,dc=com" scope=0
filter="(|(objectclass=*)(objectclass=ldapsubentry))" attrs=ALL
[time_stamp] conn=2 (Internal) op=37(1) RESULT err=0 tag=48 nentries=1 wtime=0.0000062569
optime=0.0000067203 etime=0.0000129148
[time_stamp] conn=2 (Internal) op=37(2) SRCH base="dc=example,dc=com" scope=2 filter="
(member=uid=user,dc=example,dc=com)" attrs="member"
[time_stamp] conn=2 (Internal) op=37(2) RESULT err=0 tag=48 nentries=0 wtime=0.0000058002
optime=0.0000065198 etime=0.0000123162
[time_stamp] conn=2 (Internal) op=37(3) SRCH base="dc=example,dc=com" scope=2 filter="
(uniquemember=uid=user,dc=example,dc=com)" attrs="uniquemember"
[time_stamp] conn=2 (Internal) op=37(3) RESULT err=0 tag=48 nentries=1 wtime=0.0000062123
optime=0.0000066022 etime=0.0000128104
[time_stamp] conn=2 (Internal) op=37(4) MOD dn="cn=example,dc=example,dc=com"
[time_stamp] conn=2 (Internal) op=37(5) SRCH base="cn=example,dc=example,dc=com"
scope=0 filter="(|(objectclass=\*)(objectclass=ldapsubentry))" attrs=ALL
[time_stamp] conn=2 (Internal) op=37(5) RESULT err=0 tag=48 nentries=1 wtime=0.0000061994
optime=0.0000068742 etime=0.0000130685
[time_stamp] conn=2 (Internal) op=37(4) RESULT err=0 tag=48 nentries=0 wtime=0.0002600573
optime=0.0002617786 etime=0.0005217545
[time_stamp] conn=2 (Internal) op=37(6) SRCH base="dc=example,dc=com" scope=2 filter="
(owner=uid=user,dc=example,dc=com)" attrs="owner"
[time_stamp] conn=2 (Internal) op=37(6) RESULT err=0 tag=48 nentries=0 wtime=0.000061678
optime=0.000076107 etime=0.0000137656
[time_stamp] conn=2 (Internal) op=37(7) SRCH base="dc=example,dc=com" scope=2 filter="
(seeAlso=uid=user,dc=example,dc=com)" attrs="seeAlso"
[time_stamp] conn=2 (Internal) op=37(7) RESULT err=0 tag=48 nentries=0 wtime=0.0000031789
optime=0.0000035354 etime=0.0000066978
[time_stamp] conn=2 (Internal) op=37(8) SRCH base="o=example" scope=2 filter="
(member=uid=user,dc=example,dc=com)" attrs="member"
```

```
[time_stamp] conn=2 (Internal) op=37(8) RESULT err=0 tag=48 nentries=0 wtime=0.0000030987
optime=0.0000032456 etime=0.0000063316
[time_stamp] conn=2 (Internal) op=37(9) SRCH base="o=example" scope=2 filter="
(uniquemember=uid=user,dc=example,dc=com)" attrs="uniquemember"
[time_stamp] conn=2 (Internal) op=37(9) RESULT err=0 tag=48 nentries=0 wtime=0.0000021958
optime=0.0000026676 etime=0.0000048634
[time_stamp] conn=2 (Internal) op=37(10) SRCH base="o=example" scope=2 filter="
(owner=uid=user,dc=example,dc=com)" attrs="owner"
[time_stamp] conn=2 (Internal) op=37(10) RESULT err=0 tag=48 nentries=0
wtime=0.0000022109 optime=0.00000268003 etime=00000048854
[time_stamp] conn=2 (Internal) op=37(11) SRCH base="o=example" scope=2 filter="
(seeAlso=uid=user,dc=example,dc=com)" attrs="seeAlso"
[time_stamp] conn=2 (Internal) op=37(11) RESULT err=0 tag=48 nentries=0
wtime=0.0000021786 optime=0.0000024867 etime=0.0000046522
[time_stamp] conn=2 op=37 RESULT err=0 tag=107 nentries=0 wtime=0.005147365
optime=0.005150798 etime=0.0010297858
```

访问条目和引用

当您为访问条目和引用(512)启用日志记录时，Directory 服务器在访问日志文件中具有以下记录：

```
[time_stamp] conn=306 fd=60 slot=60 connection from 127.0.0.1 to 127.0.0.1
[time_stamp] conn=306 op=0 SRCH base="dc=example,dc=com" scope=2 filter="
(description=*)" attrs=ALL
[time_stamp] conn=306 op=0 ENTRY dn="ou=Special
[time_stamp] conn=306 op=0 ENTRY dn="cn=Accounting
Managers,ou=groups,dc=example,dc=com"
[time_stamp] conn=306 op=0 ENTRY dn="cn=HR Managers,ou=groups,dc=example,dc=com"
[time_stamp] conn=306 op=0 ENTRY dn="cn=QA Managers,ou=groups,dc=example,dc=com"
[time_stamp] conn=306 op=0 ENTRY dn="cn=PD Managers,ou=groups,dc=example,dc=com"
[time_stamp] conn=306 op=0 ENTRY dn="ou=Red Hat Servers,dc=example,dc=com"
[time_stamp0] conn=306 op=0 REFERRAL
```

该示例具有日志级别 768 (512 + 256)，并显示六个条目，以及一个搜索请求在响应时返回的引用。

选项描述

options=persistent 消息表示 Directory 服务器执行持久性搜索。您可以使用持久性搜索来监控目的，并在发生更改时配置将更改返回到给定配置。

以下示例显示了包含选项描述的 512 和 4 日志级别。

```
[time_stamps] conn=1 (Internal) op=2(1)(0) SRCH
base="cn=\22dc=example,dc=com\22,cn=mapping tree,cn=config"scope=0
filter="objectclass=nsMappingTree"attrs="nsslapd-referral" options=persistent
```

每个搜索操作的统计信息

当您将 nsslapd-statlog-level 属性设置为 1 时，访问日志开始收集指标，如每个搜索操作的索引查找数和整个持续时间。

```
[time_stamps] conn=1 op=73 SRCH base="dc=example,dc=com" scope=2 filter="(cn=user_*)" attrs=ALL
[time_stamps] conn=1 op=73 STAT read index: attribute=objectclass key(eq)=referral --> count 0
[time_stamps] conn=1 op=73 STAT read index: attribute=cn key(sub)=er_ --> count 24
[time_stamps] conn=1 op=73 STAT read index: attribute=cn key(sub)=ser --> count 25
[time_stamps] conn=1 op=73 STAT read index: attribute=cn key(sub)=use --> count 25
[time_stamps] conn=1 op=73 STAT read index: attribute=cn key(sub)=^us --> count 24
[time_stamps] conn=1 op=73 STAT read index: duration 0.000010276
[time_stamps] conn=1 op=73 RESULT err=0 tag=101 nentries=24 wtime=0.00007841
```

日志记录示例显示，在搜索过滤器 (cn=useruildDefaults) 期间，Directory 服务器执行以下数据库查找数：

- 0 用于引用
- 24 for er_ key
- 25 对于 ser 键
- 25 对于 use 键
- 24 对于 ^us 键

11.1.4. 常见连接代码

目录服务器将连接代码添加到关闭日志消息中，其中包含与连接冲突相关的其他信息。

连接代码	描述
A1	客户端中止连接。

连接代码	描述
B1	遇到损坏的 BER 标签。当目录服务器收到通过线路发送的损坏的 BER 标签时，目录服务器会将 B1 连接代码记录到访问日志。BER 标签可能会因为物理层网络问题或错误的 LDAP 客户端操作而损坏，如 LDAP 客户端在接收所有请求结果前取消操作。
B2	BER 标签比 **nsslapd-maxbersize** 属性值长。
B3	遇到损坏的 BER 标签。
B4	服务器无法将响应发回到客户端。
P2	检测到关闭或损坏连接。
T1	客户端在闲置周期后不会收到您可以在 **nsslapd-idletimeout** 属性中设置的空闲周期后的结果。
T2	在 **nsslapd-ioblocktimeout** 中设置的时间后，服务器关闭了到停滞的 LDAP 客户端的连接。
U1	服务器在客户端发送未绑定请求后关闭连接。当服务器收到未绑定请求时，服务器总是关闭连接。

其他资源

- ***nsslapd-idletimeout 属性的描述***
- ***nsslapd-maxbersize 属性的描述***
- ***nsslapd-ioblocktimeout 属性的描述***

11.2. 错误日志参考

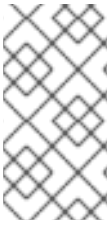
Directory 服务器错误记录目录服务器事务和操作的消息。错误日志不仅包含失败操作的错误消息，还包含有关目录服务器进程和 LDAP 任务的常规信息，如服务器启动消息、登录和搜索目录以及连接信息。

11.2.1. 错误日志记录级别

错误日志可以记录目录服务器操作的不同详情，包括不同类型的信息，具体取决于启用的日志级别。

您可以使用 cn=config 条目的 nsslapd-errorlog-level 配置属性来设置日志记录级别。

默认日志记录级别为 16384。此级别包括严重错误消息和标准记录的消息，如 LDAP 结果代码和启动消息。错误日志记录级别是可添加的。要启用复制日志记录(8192)和插件日志记录(65536)，请将 nsslapd-errorlog-level 属性设置为 73728 (8192 + 65536)。



注意

启用高级别调试日志记录可能会显著降低服务器性能。因此，只启用高调试日志记录级别，如复制(8192)，仅适用于故障排除。

表 11.1. 错误日志级别

设置	控制台名称	描述
1	跟踪函数调用	当服务器进入并退出函数时，记录一条消息。
2	数据包处理	记录服务器进程的数据包的调试信息。
4	大量追踪输出	当服务器进入并退出函数时，日志会带有额外的调试信息。
8	连接管理	记录当前连接状态，包括用于 SASL 绑定的连接方法。
16	发送和接收的数据包	打印服务器发送和接收的数据包数。
32	搜索过滤器处理	记录搜索操作调用的所有功能。
64	配置文件处理	在服务器启动时，打印每个使用的 **.conf** 配置文件（按行行）。默认情况下，目录服务器只处理 **slapd-collations.conf** 文件。
128	访问控制列表处理	提供详细的访问控制列表处理信息。
2048	日志条目解析	日志模式解析调试信息。

设置	控制台名称	描述
4096	housekeeping	记录内务线程的调试信息。
8192	复制	记录有关每个复制相关操作的详细信息，包括更新和错误，这对于调试复制问题非常重要。
16384	Default（默认）	记录 Directory 服务器始终写入错误日志的严重错误和其他消息，如服务器启动消息。无论日志级别设置是什么，错误日志都会包含这些消息。
32768	条目缓存	记录数据库条目缓存的调试信息。
65536	插件	当服务器插件调用 **slapi-log-error （）** 函数时，将条目写入日志文件。您可以使用插件日志级别进行服务器插件调试。
262144	访问控制概述	总结了有关访问服务器的信息，包含比 **128** 级别小的详细信息。当您需要访问控制处理摘要时，请使用 **262144** 值。使用 **128** 值来处理非常详细的消息。
524288	后端数据库	记录用于处理与后缀关联的数据库的调试信息。
1048576	密码策略	记录有关密码策略决策的调试信息。

其他资源

- ***nsslapd-errorlog-level 属性描述***

11.2.2. 默认错误日志内容

服务器或插件都可以将条目写入错误日志中：

- ***当服务器写入日志时，它使用以下格式：***

```
[time_stamp] - <severity_level> - <function_name> - <message>
```

服务器生成的错误日志示例：

```
[time_stamp] - NOTICE - bdb_start_autotune - found 7110616k physical memory
```

- *当插件写入日志时，它使用以下格式：*

```
[time_stamp] - <severity_level> - <plug-in_name> - <function_name> - <message>
```

插件生成的错误日志示例：

```
[time_stamp] - ERR - NSMMReplicationPlugin -
multimaster_extop_StartNSDS50ReplicationRequest - conn=19 op=3
repl="o=example.com": Excessive clock skew from supplier RUV
```

错误日志条目包含以下信息：

日志消息	描述
时间戳	时间戳格式可能会因您的本地设置而异。默认情况下启用高分辨率时间戳，以纳秒为单位。

日志消息	描述
严重性级别	严重性级别可以具有以下值： • **当服务器** 无法启动时，EMERG。 • **当服务器** 处于 critical 状态时，ALERT 必须采取可能的操作。 • 出现严重错误时 **CRIT**。 • 显示常规错误时 **ERR**。 • **警告**，表示不一定出错的警告消息。 • **当出现** 正常但出现重大条件时，不要ICE。例如，Directory 服务器会记录预期行为的通知消息。 • **INFO** 用于信息性消息，如启动、关闭、导入、导出、备份和恢复。 • **DEBUG** 用于调试级消息。详细日志记录级别，如 Trace 功能调用(1)，访问控制列表处理(**128**)和复制(**8192**)默认使用 **DEBUG** 信息。
插件名称	只有在插件将消息写入错误日志时才会显示插件名称。
功能名称	操作或插件调用的功能。
消息	operation 或 插件返回的输出。消息包含其他信息，如 LDAP 错误代码和连接信息。

您可以使用严重性级别来过滤您的日志条目。例如，要只显示 ERR 严重性为 ERR 的日志条目，请运行：

```
# grep ERR /var/log/dirsrv/slapd-instance_name/errors
[time_stamp] - ERR - no_diskspace - No enough space left on device (/var/lib/dirsrv/slapd-instance_name/db) (40009728 bytes); at least 145819238 bytes space is needed for db region files
[time_stamp] - ERR - ldbm_back_start - Failed to init database, err=28 No space left on device
[time_stamp] - ERR - plugin_dependency_startall - Failed to start database plugin ldbm database
...
```

其他资源

- 错误日志记录级别

11.2.3. 非默认错误日志内容

不同的日志记录级别返回不同的详细信息，包括服务器操作的类型。以下是默认情况下不启用的最常用错误日志记录级别。请记住，您可以组合日志记录级别。

复制(8192)

复制日志记录是要实施的最重要诊断级别之一。复制(8192)级别记录与复制和 Windows 同步相关的所有操作，包括处理供应商修改并将其写入更改日志、发送更新和更改复制协议。

当目录服务器准备或发送复制更新时，错误日志会标识它是复制或同步协议。日志还标识使用者主机和端口，以及当前的复制任务。

复制级别日志的格式如下：

```
[time_stamp] NSMMReplicationPlugin - agmt="name" (consumer_host:consumer_port):
current_task
```

以下是复制(8192)级别日志的示例，其中 {replicageneration} 表示目录服务器发送新信息，4949df6e000000010000 是复制条目的更改序列号(CSN)：

```
[time_stamp] NSMMReplicationPlugin - agmt="cn=example2_agreement" (alt:13864):
{replicageneration} 4949df6e000000010000
```

以下是向消费者发送单个条目的完整流程示例，从添加条目到更改日志，以在复制完成后释放消费者。

```
[time_stamp] - DEBUG - _csngen_adjust_local_time - gen state before
592c103d0000:1496059964:0:1
[time_stamp] - DEBUG - _csngen_adjust_local_time - gen state after
592c10e20000:1496060129:0:1
[time_stamp] - DEBUG - NSMMReplicationPlugin - ruv_add_csn_inprogress - Successfully
inserted csn 592c10e2000000020000 into pending list
[time_stamp] - DEBUG - NSMMReplicationPlugin - changelog program -
_cl5GetDBFileByReplicaName - found DB object 0x558ddfe1f720 for database
/var/lib/dirsrv/slapd-supplier_2/changelogdb/d3de3e8d-446611e7-a89886da-
6a37442d_592c0e0b000000010000.db
[time_stamp] - DEBUG - NSMMReplicationPlugin - changelog program - cl5WriteOperationTxn
- Successfully written entry with csn (592c10e2000000020000)
```

[time_stamp] - DEBUG - NSMMReplicationPlugin - changelog program - _cl5GetDBFileByReplicaName - found DB object 0x558ddfe1f720 for database /var/lib/dirsrv/slapd-supplier_2/changelogdb/d3de3e8d-446611e7-a89886da-6a37442d_592c0e0b000000010000.db
[time_stamp] - DEBUG - NSMMReplicationPlugin - csnplCommitALL: committing all csns for csn 592c10e2000000020000
[time_stamp] - DEBUG - NSMMReplicationPlugin - csnplCommitALL: processing data csn 592c10e2000000020000
[time_stamp] - DEBUG - NSMMReplicationPlugin - ruv_update_ruv - Successfully committed csn 592c10e2000000020000
[time_stamp] - DEBUG - NSMMReplicationPlugin - repl5_inc_run - agmt="cn=meTo_localhost:39001" (localhost:39001): State: wait_for_changes -> wait_for_changes
[time_stamp] - DEBUG - NSMMReplicationPlugin - repl5_inc_run - agmt="cn=meTo_localhost:39001" (localhost:39001): State: wait_for_changes -> ready_to_acquire_replica
[time_stamp] - DEBUG - NSMMReplicationPlugin - conn_connect - agmt="cn=meTo_localhost:39001" (localhost:39001) - Trying non-secure slapi_ldap_init_ext
[time_stamp] - DEBUG - NSMMReplicationPlugin - conn_connect - agmt="cn=meTo_localhost:39001" (localhost:39001) - binddn = cn=replrepl,cn=config, passwd = {AES-TUhNR0NTcUdTSWlzRFFFRkRUQm1NRVVHQ1NxR1NJYjNEUUVGRERBNEJDUmlZVFUzTnpRMk55MDBaR1ZtTXpobQ0KTWkxaE9XTTRPREpoTlMwME1EaGpabVUxWmdBQ0FRSUNBU0F3Q2dZSUtvWklodmNOQWdjd0hRWUpZSVpJQVdVRA0KQkFFcUJCRGhwMnNLcEZ2ZWE2RzEwWG10OU41Tg==}+36owal7oTmvWhxRzUqX5w==
[time_stamp] - DEBUG - NSMMReplicationPlugin - conn_cancel_linger - agmt="cn=meTo_localhost:39001" (localhost:39001) - No linger to cancel on the connection
[time_stamp] - DEBUG - _csngen_adjust_local_time - gen state before 592c10e20001:1496060129:0:1
[time_stamp] - DEBUG - _csngen_adjust_local_time - gen state after 592c10e30000:1496060130:0:1
[time_stamp] - DEBUG - NSMMReplicationPlugin - acquire_replica - agmt="cn=meTo_localhost:39001" (localhost:39001): Replica was successfully acquired.
[time_stamp] - DEBUG - NSMMReplicationPlugin - repl5_inc_run - agmt="cn=meTo_localhost:39001" (localhost:39001): State: ready_to_acquire_replica -> sending_updates
[time_stamp] - DEBUG - csngen_adjust_time - gen state before 592c10e30001:1496060130:0:1
[time_stamp] - DEBUG - NSMMReplicationPlugin - changelog program - _cl5GetDBFile - found DB object 0x558ddfe1f720 for database /var/lib/dirsrv/slapd-supplier_2/changelogdb/d3de3e8d-446611e7-a89886da-6a37442d_592c0e0b000000010000.db
[time_stamp] - DEBUG - NSMMReplicationPlugin - changelog program - _cl5PositionCursorForReplay - (agmt="cn=meTo_localhost:39001" (localhost:39001)): Consumer RUV:
[time_stamp] - DEBUG - NSMMReplicationPlugin - agmt="cn=meTo_localhost:39001" (localhost:39001): {replicageneration} 592c0e0b000000010000
[time_stamp] - DEBUG - NSMMReplicationPlugin - agmt="cn=meTo_localhost:39001" (localhost:39001): {replica 1 ldap://localhost:39001} 592c0e17000000010000 592c0e1a000100010000 00000000
[time_stamp] - DEBUG - NSMMReplicationPlugin - agmt="cn=meTo_localhost:39001" (localhost:39001): {replica 2 ldap://localhost:39002} 592c103c000000020000 592c103c000000020000 00000000
[time_stamp] - DEBUG - NSMMReplicationPlugin - changelog program - _cl5PositionCursorForReplay - (agmt="cn=meTo_localhost:39001" (localhost:39001)): Supplier RUV:
[time_stamp] - DEBUG - NSMMReplicationPlugin - agmt="cn=meTo_localhost:39001" (localhost:39001): {replicageneration} 592c0e0b000000010000

[time_stamp] - DEBUG - NSMMReplicationPlugin - agmt="cn=meTo_localhost:39001" (localhost:39001): {replica 2 ldap://localhost:39002} 592c103c000000020000 592c10e2000000020000 592c10e1
[time_stamp] - DEBUG - NSMMReplicationPlugin - agmt="cn=meTo_localhost:39001" (localhost:39001): {replica 1 ldap://localhost:39001} 592c0e1a000100010000 592c0e1a000100010000 00000000
[time_stamp] - DEBUG - agmt="cn=meTo_localhost:39001" (localhost:39001) - clcache_get_buffer - found thread private buffer cache 0x558ddf870f00
[time_stamp] - DEBUG - agmt="cn=meTo_localhost:39001" (localhost:39001) - clcache_get_buffer - _pool is 0x558ddfe294d0 _pool->pl_busy_lists is 0x558ddfab84c0 _pool->pl_busy_lists->bl_buffers is 0x558ddf870f00
[time_stamp] - DEBUG - agmt="cn=meTo_localhost:39001" (localhost:39001) - clcache_initial_anchorcsn - agmt="cn=meTo_localhost:39001" (localhost:39001) - (cscb 0 - state 0) - csnPrevMax () csnMax (592c10e2000000020000) csnBuf (592c103c000000020000) csnConsumerMax (592c103c000000020000)
[time_stamp] - DEBUG - clcache_initial_anchorcsn - anchor is now: 592c103c000000020000
[time_stamp] - DEBUG - NSMMReplicationPlugin - changelog program - agmt="cn=meTo_localhost:39001" (localhost:39001): CSN 592c103c000000020000 found, position set for replay
[time_stamp] - DEBUG - agmt="cn=meTo_localhost:39001" (localhost:39001) - clcache_get_next_change - load=1 rec=1 csn=592c10e2000000020000
[time_stamp] - DEBUG - NSMMReplicationPlugin - repl5_inc_result_threadmain - Starting
[time_stamp] - DEBUG - NSMMReplicationPlugin - repl5_inc_result_threadmain - Read result for message_id 0
[time_stamp] - DEBUG - NSMMReplicationPlugin - replay_update - agmt="cn=meTo_localhost:39001" (localhost:39001): Sending add operation (dn="cn=user,ou=People,dc=example,dc=com" csn=592c10e2000000020000)
[time_stamp] - DEBUG - NSMMReplicationPlugin - repl5_inc_result_threadmain - Read result for message_id 0
[time_stamp] - DEBUG - NSMMReplicationPlugin - replay_update - agmt="cn=meTo_localhost:39001" (localhost:39001): Consumer successfully sent operation with csn 592c10e2000000020000
[time_stamp] - DEBUG - NSMMReplicationPlugin - repl5_inc_result_threadmain - Read result for message_id 0
[time_stamp] - DEBUG - agmt="cn=meTo_localhost:39001" (localhost:39001) - clcache_adjust_anchorcsn - agmt="cn=meTo_localhost:39001" (localhost:39001) - (cscb 0 - state 1) - csnPrevMax (592c10e2000000020000) csnMax (592c10e2000000020000) csnBuf (592c10e2000000020000) csnConsumerMax (592c10e2000000020000)
[time_stamp] - DEBUG - agmt="cn=meTo_localhost:39001" (localhost:39001) - clcache_load_buffer - rc=-30988
[time_stamp] - DEBUG - NSMMReplicationPlugin - send_updates - agmt="cn=meTo_localhost:39001" (localhost:39001): No more updates to send (cl5GetNextOperationToReplay)
[time_stamp] - DEBUG - NSMMReplicationPlugin - repl5_inc_waitfor_async_results - 0 5
[time_stamp] - DEBUG - NSMMReplicationPlugin - repl5_inc_result_threadmain - Read result for message_id 0
[time_stamp] - DEBUG - NSMMReplicationPlugin - repl5_inc_result_threadmain - Read result for message_id 0
[time_stamp] - DEBUG - NSMMReplicationPlugin - repl5_inc_result_threadmain - Read result for message_id 5
[time_stamp] - DEBUG - NSMMReplicationPlugin - repl5_inc_result_threadmain - Result 1, 0, 0, 5, (null)
[time_stamp] - DEBUG - NSMMReplicationPlugin - repl5_inc_result_threadmain - Read result for message_id 5
[time_stamp] - DEBUG - NSMMReplicationPlugin - repl5_inc_waitfor_async_results - 5 5
[time_stamp] - DEBUG - NSMMReplicationPlugin - repl5_inc_result_threadmain exiting

```
[time_stamp] - DEBUG - agmt="cn=meTo_localhost:39001" (localhost:39001) -
clcache_return_buffer - session end: state=5 load=1 sent=1 skipped=0 skipped_new_rid=0
skipped_csn_gt_cons_maxcsn=0 skipped_up_to_date=0 skipped_csn_gt_ruv=0
skipped_csn_covered=0
[time_stamp] - DEBUG - NSMMReplicationPlugin -
consumer_connection_extension_acquire_exclusive_access - conn=4 op=3 Acquired
consumer connection extension
[time_stamp] - DEBUG - NSMMReplicationPlugin -
multimaster_extop_StartNSDS50ReplicationRequest - conn=4 op=3
repl="dc=example,dc=com": Begin incremental protocol
[time_stamp] - DEBUG - csngen_adjust_time - gen state before 592c10e30001:1496060130:0:1
[time_stamp] - DEBUG - csngen_adjust_time - gen state after 592c10e40001:1496060130:1:1
[time_stamp] - DEBUG - NSMMReplicationPlugin - replica_get_exclusive_access - conn=4
op=3 repl="dc=example,dc=com": Acquired replica
[time_stamp] - DEBUG - NSMMReplicationPlugin - release_replica -
agmt="cn=meTo_localhost:39001" (localhost:39001): Successfully released consumer
[time_stamp] - DEBUG - NSMMReplicationPlugin - conn_start_linger -
agmt="cn=meTo_localhost:39001" (localhost:39001) - Beginning linger on the connection
[time_stamp] - DEBUG - NSMMReplicationPlugin - repl5_inc_run -
agmt="cn=meTo_localhost:39001" (localhost:39001): State: sending_updates ->
wait_for_changes
[time_stamp] - DEBUG - NSMMReplicationPlugin -
multimaster_extop_StartNSDS50ReplicationRequest - conn=4 op=3
repl="dc=example,dc=com": StartNSDS90ReplicationRequest: response=0 rc=0
[time_stamp] - DEBUG - NSMMReplicationPlugin -
consumer_connection_extension_relinquish_exclusive_access - conn=4 op=3 Relinquishing
consumer connection extension
[time_stamp] - DEBUG - NSMMReplicationPlugin -
consumer_connection_extension_acquire_exclusive_access - conn=4 op=4 Acquired
consumer connection extension
[time_stamp] - DEBUG - NSMMReplicationPlugin - replica_relinquish_exclusive_access -
conn=4 op=4 repl="dc=example,dc=com": Released replica held by locking_purl=conn=4 id=3
[time_stamp] - DEBUG - NSMMReplicationPlugin -
consumer_connection_extension_relinquish_exclusive_access - conn=4 op=4 Relinquishing
consumer connection extension
```

Plug-in (65536)

插件(65536)级别记录了插件的名称，以及插件调用的所有功能。

插件级别日志的格式如下：

```
[time_stamp] plug-in_name - message
[time_stamp] - function - message
```

返回的信息可以包含数百个行，因为目录服务器会处理每个步骤。确切记录的信息取决于插件本身。在以下示例中，ACL 插件包含连接和操作号：

```
[time_stamp] - DEBUG - NSACLPlugin - acl_access_allowed - conn=15 op=1 (main): Allow
search on entry(cn=replication,cn=config): root user
```

-

配置文件处理(64)

配置文件处理日志级别会经过服务器使用的每个 .conf 文件，并在服务器启动时打印每一行。您可以使用 64 日志级别来调试服务器常规配置外文件的任何问题。默认情况下，只有 slapd-collations.conf 文件（其中包含国际语言集的配置）可用。

配置文件处理(64)级别）的示例：

```
[time_stamp] - DEBUG - collation_read_config - Reading config file /etc/dirsrv/slapd-
supplier_1/slapd-collations.conf
[time_stamp] - DEBUG - collation-plugin - collation_read_config - line 16: collation "" "" "" 1 3
2.16.840.1.113730.3.3.2.0.1 default
[time_stamp] - DEBUG - collation-plugin - collation_read_config - line 17: collation ar "" "" 1 3
2.16.840.1.113730.3.3.2.1.1 ar
[time_stamp] - DEBUG - collation-plugin - collation_read_config - line 18: collation be "" "" 1 3
2.16.840.1.113730.3.3.2.2.1 be be-BY
...
```

访问控制列表处理(128)和访问控制摘要(262144)

其他日志级别不包含连接号(conn)和操作号(op)的 ACI 日志记录级别记录信息。访问控制列表处理(128)显示绑定和任何其他操作过程中调用的一系列功能。访问控制摘要(262144)记录插件的名称、用户的绑定 DN、执行或尝试操作以及应用的 ACI。

访问控制概述示例(262144)级别：

```
[time_stamp] - DEBUG - NSACLPlugin - acllist_init_scan - Failed to find root for base:
cn=features,cn=config
[time_stamp] - DEBUG - NSACLPlugin - acllist_init_scan - Failed to find root for base:
cn=config
[time_stamp] - DEBUG - NSACLPlugin - acl_access_allowed - ## conn=6 op=1
binddn="cn=user,ou=people,dc=example,dc=com"
[time_stamp] - DEBUG - NSACLPlugin -                RESOURCE INFO STARTS
[time_stamp] - DEBUG - NSACLPlugin -    Client DN: cn=user,ou=people,dc=example,dc=com
[time_stamp] - DEBUG - NSACLPlugin -    resource type:256(search target_DN )
[time_stamp] - DEBUG - NSACLPlugin -    Slapi_Entry DN: cn=features,cn=config
[time_stamp] - DEBUG - NSACLPlugin -    ATTR: objectClass
[time_stamp] - DEBUG - NSACLPlugin -    rights:search
[time_stamp] - DEBUG - NSACLPlugin -                RESOURCE INFO ENDS
[time_stamp] - DEBUG - NSACLPlugin - acl__scan_for_acis - Num of ALLOW Handles:0, DENY
handles:0
[time_stamp] - DEBUG - NSACLPlugin - print_access_control_summary - conn=6 op=1 (main):
Deny search on entry(cn=features,cn=config).attr(objectClass) to
cn=user,ou=people,dc=example,dc=com: no aci matched the resource
```

其他日志记录级别

许多其他日志记录级别具有与插件日志级别类似的输出格式。唯一的区别是在记录的内部操作中。

日志记录级别，如 Heavy trace output (4)、访问控制列表处理(128)、模式解析(2048)和内务(4096)级别，在目录服务器执行不同操作时记录调用的功能。另外，当目录服务器调用这些功能时，错误日志写入。

11.3. 审计日志参考

审计日志记录对每个数据库和服务器配置所做的更改。默认不启用此日志类型。如果启用审计日志记录，Directory 服务器只记录对审计日志文件成功的操作。但是，如果您启用审计失败日志记录，您可以将失败的操作记录到单独的文件中。

与错误和访问日志不同，审计日志不会记录对服务器实例的访问，因此不会记录对数据库进行搜索。

审计日志的格式与 access 和 error 日志格式不同。目录服务器在 LDIF 语句中记录审计日志中的操作：

```
timestamp: date
dn: modified_entry
changetype: action
action:attribute
attribute:new_value
-
replace: modifiersname
modifiersname: dn
-
replace: modifytimestamp
modifytimestamp: date
-
```

有关 LDIF 文件和格式的详情，请参阅 LDAP 数据交换格式

审计日志示例：

```
... modifying an entry ...
time: 20200108181429
dn: uid=scarter,ou=people,dc=example,dc=com
changetype: modify
replace: userPassword
userPassword: {SSHA}8EcJhJolgBgY/E5j8JiVoj6W3BLyj9Za/rCPOw==
-
```

```
replace: modifiersname
modifiersname: cn=Directory Manager
-
replace: modifytimestamp
modifytimestamp: 20200108231429Z
-

... sending a replication update ...
time: 20200109131811
dn: cn=example2,cn=replica,cn="dc=example,dc=com",cn=mapping tree,cn=config
changetype: modify
replace: nsds5BeginReplicaRefresh
nsds5BeginReplicaRefresh: start
-
replace: modifiersname
modifiersname: cn=Directory Manager
-
replace: modifytimestamp
modifytimestamp: 20200109181810Z
-
```

其他资源

- 配置日志文件

11.4. 审计失败日志参考

如果启用失败的审计日志记录，Directory 服务器将启动仅向审计失败日志文件记录对服务器实例所做的更改。

审计失败日志的格式与审计日志相同，看起来像 LDIF 语句，默认情况下不启用。

其他资源

- 配置日志文件

11.5. 安全日志参考

安全日志记录各种安全事件，包括：

- 身份验证事件

- 授权问题
- DoS 和 TCP 攻击

目录服务器将安全日志与其他日志文件一起存储在 /var/log/dirsrv/slapd-instance_name/ 目录中。与具有所有信息的访问日志相比，安全日志不会快速轮转，且消耗较少的磁盘资源，但需要昂贵的解析来获取安全数据。

安全日志采用 JSON 格式，并允许其他工具执行日志的复杂解析。您无法更改日志格式或为安全日志设置日志级别。

安全日志示例：

```
{ “date”: “[time_stamp] “, “utc_time”: “1684155510.154562500", “event”: “BIND_SUCCESS”, “dn”: “cn=directory manager”, “bind_method”: “LDAPI”, “root_dn”: true, “client_ip”: “local”, “server_ip”: “\/run\/slapd-instance_name.socket”, “ldap_version”: 3, “conn_id”: 1, “op_id”: 0, “msg”: “” }
{ “date”: “[time_stamp] “, “utc_time”: “1684155510.163790695", “event”: “BIND_SUCCESS”, “dn”: “cn=directory manager”, “bind_method”: “LDAPI”, “root_dn”: true, “client_ip”: “local”, “server_ip”: “\/run\/slapd-instance_name.socket”, “ldap_version”: 3, “conn_id”: 2, “op_id”: 0, “msg”: “” }
{'date': '[time_stamp]', 'utc_time': '168485945', 'event': 'BIND_FAILED', 'dn': 'uid=mark,ou=people,dc=example,dc=com', 'bind_method': 'SIMPLE', 'root_dn': 'false', 'client_ip': '127.0.0.1', 'server_ip': '127.0.0.1', 'conn_id': '2', 'op_id': '1', 'msg': 'INVALID_PASSWORD'}
{'date': '[time_stamp]', 'utc_time': '168499999', 'event': 'BIND_FAILED', 'dn': 'uid=mike,ou=people,dc=example,dc=com', 'bind_method': 'SIMPLE', 'root_dn': 'false', 'client_ip': '127.0.0.1', 'server_ip': '127.0.0.1', 'conn_id': '7', 'op_id': '1', 'msg': 'NO_SUCH_ENTRY'}
{"date": "[time_stamp]", "utc_time": 1657907429, "event": "TCP_ERROR", "client_ip": "::1", "server_ip": "::1", "ldap_version": 3, "conn_id": 1, "msg": "Bad Ber Tag or uncleanly closed connection - B1"}
```

日志示例显示，两个绑定到服务器已成功，两个绑定失败，一个事件是一个 TCP 错误。

另外，当您使用 pre-bind 身份验证插件为用户帐户配置双因素身份验证时，安全日志记录绑定方法，例如：

```
{ "date": "[time_stamp] ", "utc_time": "1709327649.232748932", "event": "BIND_SUCCESS", "dn": "uid=djoe,ou=people,dc=example,dc=com", "bind_method": "SIMPLE\/MFA", "root_dn": false, "client_ip": "::1", "server_ip": "::1", "ldap_version": 3, "conn_id": 1, "op_id": 0, "msg": "" }
```

请注意，对于 secutiry 日志来记录此类消息，如果绑定是这个插件的一部分，则 pre-bind 身份验证插件必须使用 SLAPI API 设置此插件的一部分。

其他资源

- *配置日志文件*

11.6. LDAP 结果代码

目录服务器使用以下 LDAP 结果对日志文件进行编码：

十进制值	十六进制值	Constants
0	0x00	LDAP_SUCCESS
1	0x01	LDAP_OPERATIONS_ERROR
2	0x02	LDAP_PROTOCOL_ERROR
3	0x03	LDAP_TIMELIMIT_EXCEEDED
4	0x04	LDAP_SIZELIMIT_EXCEEDED
5	0x05	LDAP_COMPARE_FALSE
6	0x06	LDAP_COMPARE_TRUE
7	0x07	LDAP_AUTH_METHOD_NOT_SUPPORTED LDAP_STRONG_AUTH_NOT_SUPPORTED
8	0x08	LDAP_STRONGER_AUTH_REQUIRED LDAP_STRONG_AUTH_REQUIRED
9	0x09	LDAP_PARTIAL_RESULTS
10	0x0a	LDAP_REFERRAL (LDAPv3)
11	0x0b	LDAP_ADMINLIMIT_EXCEEDED

十进制值	十六进制值	Constants
12	0x0c	LDAP_UNAVAILABLE_CRITICAL_EXTENSION
13	0x0d	LDAP_CONFIDENTIALITY_REQUIRED
14	0x0e	LDAP_SASL_BIND_IN_PROGRESS
16	0x10	LDAP_NO_SUCH_ATTRIBUTE
17	0x11	LDAP_UNDEFINED_TYPE
18	0x12	LDAP_INAPPROPRIATE_MATCHING
19	0x13	LDAP_CONSTRAINT_VIOLATION
20	0x14	LDAP_TYPE_OR_VALUE_EXISTS
21	0x15	LDAP_INVALID_SYNTAX
32	0x20	LDAP_NO_SUCH_OBJECT
33	0x21	LDAP_ALIAS_PROBLEM
34	0x22	LDAP_INVALID_DN_SYNTAX
35	0x23	LDAP_IS_LEAF （在 LDAPv3 中使用）
36	0x24	LDAP_ALIAS_DEREF_PROBLEM
48	0x30	LDAP_INAPPROPRIATE_AUTH
49	0x31	LDAP_INVALID_CREDENTIALS
50	0x32	LDAP_INSUFFICIENT_ACCESS
51	0x33	LDAP_BUSY
52	0x34	LDAP_UNAVAILABLE

十进制值	十六进制值	Constants
53	0x35	LDAP_UNWILLING_TO_PERFORM
54	0x36	LDAP_LOOP_DETECT
60	0x3c	LDAP_SORT_CONTROL_MISSING
61	0x3d	LDAP_INDEX_RANGE_ERROR
64	0x40	LDAP_NAMING_VIOLATION
65	0x41	LDAP_OBJECT_CLASS_VIOLATION
66	0x42	LDAP_NOT_ALLOWED_ON_NONLEAF
67	0x43	LDAP_NOT_ALLOWED_ON_RDN
68	0x44	LDAP_ALREADY_EXISTS
69	0x45	LDAP_NO_OBJECT_CLASS_MODS
70	0x46	LDAP_RESULTS_TOO_LARGE（用于 CLDAP 的保留）
71	0x47	LDAP_AFFECTS_MULTIPLE_DSAS
76	0x4C	LDAP_VIRTUAL_LIST_VIEW_ERROR
80	0x50	LDAP_OTHER
81	0x51	LDAP_SERVER_DOWN
82	0x52	LDAP_LOCAL_ERROR
83	0x53	LDAP_ENCODING_ERROR
84	0x54	LDAP_DECODING_ERROR
85	0x55	LDAP_TIMEOUT

十进制值	十六进制值	Constants
86	0x56	LDAP_AUTH_UNKNOWN
87	0x57	LDAP_FILTER_ERROR
88	0x58	LDAP_USER_CANCELLED
89	0x59	LDAP_PARAM_ERROR
90	0x5A	LDAP_NO_MEMORY
91	0x5B	LDAP_CONNECT_ERROR
92	0x5C	LDAP_NOT_SUPPORTED
93	0x5D	LDAP_CONTROL_NOT_FOUND
94	0x5E	LDAP_MORE_RESULTS_TO_RETURN
95	0x5F	LDAP_MORE_RESULTS_TO_RETURN
96	0x60	LDAP_CLIENT_LOOP
97	0x61	LDAP_REFERRAL_LIMIT_EXCEEDED
118	0x76	LDAP_CANCELLED